A EVOLUÇÃO E O FUTURO DA CIBERGUERRA: UM ESTUDO APROFUNDADO SOBRE A FRANÇA

THE EVOLUTION AND FUTURE OF CYBER WAR: AN IN-DEPTH STUDY OF FRANCE

DOI: 10.5380/cg.v13i1.92715

Natalia Diniz Schwether[1]

Resumo

O artigo entende a guerra do futuro a partir da lente de análise da cibernética e centra sua análise no caso francês, uma das dez nações mais poderosas no ciberespaço do mundo. O país, nas últimas décadas, atualizou tanto os seus documentos estratégicos quanto reorganizou o seu aparato de segurança e defesa cibernética. O intuito é, então, responder ao questionamento geral: como a França tem se organizado para travar a guerra do futuro? E, de forma mais específica: qual o papel da cibernética na preparação desse país? Para tanto, realiza-se um estudo de caso, detendo como principal estratégia de pesquisa a exploração, em especial, de fontes primárias e de documentos oficiais, nos quais são identificados os elementos centrais da política cibernética francesa e as instituições indispensáveis para sua operação. O principal achado diz respeito ao modelo de governança francês do ciberespaço, no qual há uma tentativa de separar as missões e as capacidades ofensivas das defensivas.
Palavras-Chave: Guerra do Futuro; Cibernética; Estratégia; Estudo de Caso; França.

Abstract

The article understands the war of the future from the analytical lens of cybernetics and focuses its analysis on the French case, one of the ten most powerful nations in cyberspace in the world. This country, in recent decades, has updated both its strategic documents and reorganized its cyber security and defense apparatus. The aim of the present study is, then, to answer the general question: how has France organized itself to fight the war of the future? And, more specifically: what is the role of cybernetics in preparing this country? To this end, it carries out a case study, whose main research strategy is the exploration of primary sources and official documents, in which we find the central elements of French cyber policy and the essential institutions for its operation. The main

[1] Universidade Federal de Santa Catarina, natidiniz@gmail.com, ORCID: https://orcid.org/0000-0002-8022-237X. O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

finding concerns the French cyberspace governance model, in which there is an attempt to separate offensive and defensive missions and capabilities.
Keywords: Future War; Cybernetics; Strategy; Case study; France.

1. INTRODUÇÃO

O termo 'futuro' possui definição ampla e subjetiva, para o qual diferentes estudos empregam distintas métricas e prazos. As mudanças constantes e o rápido avanço da tecnologia tornam o estudo do futuro da guerra um problema complexo, o qual exige antecipação a fim de garantir uma melhor capacidade de inovar e adaptar as abordagens, bem como de explorar as oportunidades e proteger as vulnerabilidades.

No ambiente operacional futuro, particularmente instável, aspectos como: as operações em multidomínio, as tecnologias emergentes e disruptivas, a urbanização dos conflitos e as ações intensivas no ciberespaço ganham relevância. A expansão do campo de batalha para além das escalas geográficas tradicionais, bem como a variedade de domínios e meios disponíveis para emprego, impactam na formulação de estratégias e no planejamento das missões. Nesse sentido, a organização do setor cibernético, em particular o da França, é uma fonte de reflexão (VIDELIN, 2018).

A França, membro permanente do Conselho de Segurança das Nações Unidas, potência nuclear, uma das principais potências militares da União Europeia[2] e a nona nação mais poderosa no ciberespaço[3], foi o caso eleito para a presente análise, dado o seu empenho em adaptar suas forças convencionais para lidar, também, com as ameaças cibernéticas (SIMÃO, 2021).

A instituição militar francesa, historicamente, tem optado por explorar a totalidade de suas capacidades, com uma doutrina que encoraja a movimentação rápida, a agilidade e a assunção de riscos, sobretudo, após o fim da conscrição obrigatória, na década de 1990. A ênfase em forças expedicionárias, flexíveis e com alta capacidade, tem direcionado, ao longo do tempo, os investimentos e o foco das operações (SHURKIN, 2022, 2023).

Na esteira desse pensamento, as capacidades de alta intensidade e a atuação conjunta das forças têm sido priorizadas (SHURKIN, 2022). O ciberespaço e a guerra em rede, igualmente, recebem especial atenção. Em termos de cibersegurança, o país agiu rápido e adotou ações bastante conscientes destinadas a dotar sua infraestrutura cibernética e a garantir segurança aos

[2] Conforme os dados do SIPRI (2022) o investimento francês em defesa é, juntamente com a Alemanha, o mais elevado da União Europeia.
[3] Conforme os dados do National Cyber Power Index (2022) os dez Estados mais completos no que tange o poder cibernético são: Estados Unidos, China, Rússia, Reino Unido, Austrália, Países Baixos, Coréia do Sul, Vietnã, França e Irã.

seus cidadãos, com a criação, por exemplo, da Agência Nacional de Segurança de Sistemas de Informação (ANSSI) (VIDELIN, 2018).

No campo militar, o tema apareceu pela primeira vez no Livro Branco de 2008, e, desde então, tem sido possível distinguir progressos tanto na vertente doutrinária, quanto institucional (VIDELIN, 2018). Cita-se a criação, em janeiro de 2017, de um comando operacional cibernético encarregado de defender as redes militares e infraestruturas críticas.

O Comando Cibernético, sob autoridade do Chefe do Estado Maior das Forças Armadas, possui um lugar especial na estratégia de defesa cibernética francesa, sendo responsável, também, pela condução das operações militares no ciberespaço (PEZARD, SHURKIN, OCHMANEK, 2021).

Frente a isso, o presente estudo de caso se propõe a responder ao seguinte questionamento geral: como a França tem se organizado para travar a guerra do futuro? E, de forma mais específica: qual o papel da cibernética na preparação do país?

Para responder a tais questionamentos, alguns conceitos são considerados chaves, como: ciberespaço e a distinção entre segurança cibernética e defesa cibernética. O ciberespaço corresponde, suscintamente, ao ambiente virtual, no qual os meios de comunicação possibilitam a interconexão mundial. É o domínio onde ocorrem as operações cibernéticas (SHELDON, 2011).

A segurança cibernética, por sua vez, se destina à proteção da sociedade, do governo e de empresas de ameaças no ciberespaço, as quais podem assumir as mais variadas facetas (física, social, financeira, política, educacional, entre outras). Já a defesa cibernética está diretamente relacionada com as operações e táticas militares para o ciberespaço, isto é: as forças armadas são as responsáveis por conduzir as ações de prevenção ou resposta a ataques (LISBOA, OLIVEIRA, 2022).

De mais a mais, a principal estratégia de pesquisa eleita pelo presente artigo foi o exame criterioso de fontes primárias, dentre elas as edições de 2008 e 2013 do Livro Branco, e as Revisões de Defesa e Segurança Nacional, 2017 e 2022, para a depreensão da grande estratégia francesa. Em soma, utilizou-se de documentos elaborados especificamente para o ciberespaço, como a Estratégia Nacional de Segurança Digital, de 2015, e a Revisão Estratégica de Ciberdefesa, de 2018. O estudo apoia-se, também, em fontes secundárias que discutem os temas de interesse.

A análise das prioridades estratégicas francesas nos permite traçar a evolução do pensamento na área, com foco para a atual organização do setor cibernético. O estudo justifica-se ao analisar um modelo distinto de organização e governança do ciberespaço, em que há a separação das missões e capacidades ofensivas das missões e capacidades defensivas, com o que, ao final, é possível tecer considerações práticas a respeito dos benefícios e prejuízos de tal modelo.

2. GRANDE ESTRATÉGIA

Os documentos estratégicos elaborados nas últimas décadas sugerem princípios comuns na doutrina e na tomada de decisão francesa. Embora possam ter sido formulados de maneiras distintas, três deles chamam a atenção: capacidade nuclear, proteção dos interesses nacionais e indústria de defesa (PEZARD, SHURKIN, OCHMANEK, 2021).

Em 2008, foi publicado o primeiro Livro Branco francês em que parlamentares foram consultados na formulação das estratégias, quinze anos após a edição anterior, e em um mundo drasticamente modificado, "não necessariamente mais perigoso, mas certamente mais imprevisível, mais instável, mais contraditório [...]" (RÉPUBLIQUE FRANÇAISE, 2008).

O Livro estabeleceu como principal ambição francesa a capacidade de antecipar, reagir e influenciar o ambiente internacional, e inovou ao traçar uma estratégia de defesa e de segurança nacional. O anseio de poder intervir em qualquer lugar a qualquer tempo implicou à França investir em uma série de domínios e capacidades sofisticadas, sejam elas de inteligência, espacial ou cibernética, para além de manter a sua dissuasão nuclear (PEZARD, SHURKIN, OCHMANEK, 2021).

No tocante ao ciberespaço, o Livro Branco de 2008 permitiu que a França desse um passo decisivo ao, já naquela oportunidade, considerá-lo como um ambiente propício a ameaças e tentativas de ataques. Nele, afirmou-se, ainda, ser inevitável uma mudança de mentalidade e de ímpeto governamental para a alternância de uma estratégia de defesa passiva para ativa, na qual se combinasse a proteção dos sistemas, a reação permanente e rápida e a ação ofensiva (RÉPUBLIQUE FRANÇAISE, 2008).

Tendo em vista a natureza imediata e quase imprevisível dos ataques cibernéticos, o Livro considerou crucial que a França detivesse uma capacidade de gestão de crise e pós-crise. Nessa seara, anunciou a criação de uma agência nacional para lidar com os ataques cibernéticos e proteger os sistemas de informação do Estado e das infraestruturas críticas (RÉPUBLIQUE FRANÇAISE, 2008).

E, em se tratando de um novo campo de ação militar, propôs-se no referido documento que o país desenvolvesse a capacidade de combate no ciberespaço. "No domínio cibernético, mais do que em qualquer outro ambiente, para se defender, é preciso saber atacar" (RÉPUBLIQUE FRANÇAISE, 2008, p. 53). Surge, neste momento, o conceito de *Lutte Informatique Offensive (LIO)*, em que, para além das técnicas de neutralização dos adversários, também passariam a ser concebidos modos ofensivos de ação.

Para o horizonte de 2025, o Livro Branco de 2008 prospectou, ainda, a importância crescente de operações combinadas com ações no ciberespaço. As Forças Armadas deveriam, portanto, estar

prontas para conduzir ações no amplo espectro, o que careceria de investimentos, principalmente, na definição de um quadro de profissionais, no desenvolvimento de ferramentas especializadas, na formulação de uma doutrina e na implementação de um treinamento adequado (RÉPUBLIQUE FRANÇAISE, 2008).

Mais tarde, na atualização do Livro Branco, apresentada em 2013, foram reforçadas as três prioridades indissociáveis da estratégia de defesa francesa: proteção, dissuasão e intervenção. E, como já identificadas na versão anterior, as ameaças relacionadas à expansão e ao uso generalizado do ciberespaço, intencionais ou não, permaneceram sendo consideradas uma questão de atenção, muito em virtude do rápido desenvolvimento das infraestruturas digitais (RÉPUBLIQUE FRANÇAISE, 2013).

O documento, contudo, foi além, e com vistas à alta probabilidade e ao alto impacto potencial de um ataque cibernético, estabeleceu que: “um ataque contra os sistemas de informação nacionais em um cenário de guerra informacional constitui, para a França e seus parceiros europeus, uma ameaça de primeira importância” (RÉPUBLIQUE FRANÇAISE, 2013, p. 45). Logo, proteger o território e os cidadãos contra os ciberataques tornou-se uma prioridade estratégica.

Outrossim, o documento reafirmou a importância de as ações coercitivas serem realizadas de maneira coordenada nos cinco domínios - terra, ar, mar, espaço e ciberespaço. Em específico para o ciberespaço, projetou, para 2025, o aprimoramento da capacidade e a sua interrelação com o campo da inteligência, em prol de uma organização operacional integrada e adaptada às características do espaço de batalha (RÉPUBLIQUE FRANÇAISE, 2013).

Destaca-se que no caso francês a materialização da estratégia ocorre por meio da Lei de Programação Militar (LPM), um projeto plurianual aprovado pelo Parlamento. E, em conformidade com as tendências indicadas até aquela ocasião, a Lei n.º 2013-1168, de dezembro de 2013, relativa aos anos de 2014 a 2019, ampliou o orçamento para a aquisição de novas soluções em segurança cibernética, assim como previu dobrar o efetivo dedicado ao domínio cibernético no Ministério das Forças Armadas. Desta maneira, o ciberespaço mostrou ser uma preocupação partilhada por diferentes partidos políticos (MOLNÁR, 2019).

A centralidade do tema ganhou espaço, igualmente, naquele que se tornaria o documento orientador da política de segurança e defesa francesa. Sob incumbência do ministro das Forças Armadas, publicada em julho de 2017, a *Revue stratégique de defense et de sécurité nationale*, abordou as profundas transformações do ambiente estratégico, com ênfase para o desenvolvimento tecnológico, responsável por impor novos desafios aos sistemas tradicionais de defesa e segurança (RÉPUBLIQUE FRANÇAISE, 2017).

Frente a isso, o documento propôs atingir um modelo armado que fosse completo e equilibrado, ou seja, que assegurasse uma postura permanente de dissuasão, segurança e

proteção do território em todos os domínios. Além disso, frisou a importância de manter o alto desempenho da base industrial e tecnológica de defesa, como condição para autonomia do país (RÉPUBLIQUE FRANÇAISE, 2017). Em relação ao ciberespaço reforçou que:

> [no] ciberespaço, certos ataques podem ser considerados como uma agressão armada, devido à sua escala e gravidade. Um grande ataque cibernético pode, pelos danos que pode causar, justificar a invocação de legítima defesa sob o Artigo 51 da Carta da ONU (RÉPUBLIQUE FRANÇAISE, 2017, p. 33).

Na LPM 2019-2025, mais uma vez, se traduziu de maneira concreta o descrito no documento estratégico, ao dar ênfase ao combate às ciber ameaças, aos programas tecnológicos e à excelência na inovação. Na Lei nº 2018-607, cibernética e a inteligência foram consideradas as áreas triunfantes, sendo direcionados 1,6 milhões de euros para o domínio cibernético (FILIPPONE, 2018, PEZARD, SHURKIN, OCHMANEK, 2021).

Contudo, a mudança acelerada do ambiente estratégico e uma aposta na modernização das Forças como principal resposta às novas realidades, fez com que fosse necessária uma revisão antecipada da estratégia. O documento estratégico, *Actualisation Stratégique*, de 2021, confirmou as tendências identificadas até então, porém, deu destaque às ameaças híbridas, à ação deliberada de manipulação da informação e à vulnerabilidade dos dados. “O ciber e o espaço são agora campos assumidos de rivalidade estratégica” (MINISTÈRE DES ARMÉES, 2021a, p. 18).

Com isso, a adaptação da estratégia teve como foco as áreas de cibernética, espacial e Inteligência Artificial (IA). A Atualização confirmou a aposta francesa em um processo de modernização militar, com vistas à força armada completa, ágil e eficiente, bem como à superioridade estratégica e tecnológica do país. Além disso, apontou a necessária adaptação da doutrina e dos procedimentos militares, o reforço da cooperação entre os ramos das Forças, e o desenvolvimento de parcerias no ambiente internacional (MINISTÈRE DES ARMÉES, 2021a).

Em vista disso, projetou a criação de um Comando de Guerra do Futuro, para acompanhar as inovações e contribuir na coordenação das aquisições atento às necessidades futuras. Além disso, se voltou à modernização e à ampliação dos treinamentos e simulações, especialmente àqueles direcionados aos postos de comando (TOUJOUSE, 2023).

Mais recentemente, em 2022, foi apresentada a *Revue Nationale Stratégique*, o documento trouxe ao cerne da análise o regresso de uma guerra de alta intensidade em solo europeu, a qual aliada a outros fatores[4] representam “uma mudança estratégica” (RÉPUBLIQUE FRANÇAISE, 2022, p. 7), responsável por renovar tensões, consolidar parcerias e acelerar a modernização da defesa.

[4] Dentre eles a pandemia de coronavírus (COVID-19).

O documento identificou a sofisticação da capacidade cibernética ofensiva como 'sem precedentes', além de um desafio estratégico a ser abordado. Definiu, ainda, que o esforço deveria estar concentrado na melhoria da resiliência cibernética[5]. "Fortalecer o nível de cibersegurança é essencial para preparar o país para mais ameaças" (RÉPUBLIQUE FRANÇAISE, 2022, p. 37), de forma que a mobilização frente aos ataques seja ágil, envolva todas as esferas do Estado e internacionais e reduza o impacto e a duração dos incidentes.

Paralelamente, investimentos a longo prazo buscariam aprimorar a resiliência cibernética, sendo o foco a prevenção e a assistência às vítimas, além de erguer, em âmbito nacional e europeu, uma indústria competitiva de ciberdefesa, bem como uma estrutura comum de gerenciamento de crises. "A resiliência da França depende da de seus parceiros europeus e internacionais, da mesma maneira que a segurança e a estabilidade do ciberespaço" (RÉPUBLIQUE FRANÇAISE, 2022, p. 38).

A mais nova LPM, para o período entre 2024 e 2030, prevê um aumento de 36% no orçamento das Forças, dando continuidade a projetos como o sistema CAESAR de artilharia, a modernização do carro de combate LECLERC, através do programa Titan e ao sistema de comunicação SICS, que visa maior conectividade e unidades mais colaborativas (TOUJOUSE, 2023, SHURKIN, 2022, 2023). Não obstante, considera-se que áreas como a defesa antiaérea, a missilística e a cibernética, ainda prioritárias, demandam maior orçamento[6] (MANACH, 2023).

3. ESTRATÉGIA E DOUTRINA PARA O CIBERESPAÇO

A França publicou a sua primeira estratégia direcionada ao ciberespaço em 2011. A *Défense et sécurité des systémes d'information* estabeleceu quatro objetivos estratégicos e sete eixos de esforço, para um ambiente que foi considerado "a nova torre de Babel [...] o novo Thermopylae", um lugar de compartilhamento de culturas e de confronto. De forma bastante enxuta, o documento não estabeleceu caminhos futuros a serem percorridos, voltando-se a uma conscientização da importância do novo domínio e a uma apresentação do seu estado da arte (RÉPUBLIQUE FRANÇAISE, 2011).

Em 2015, a publicação da *Strategie Nationale pour la Sécurité Numérique* demarcou uma mudança de abordagem. Se até aquele momento a França mantinha uma visão técnico-militar, com foco na proteção e na resiliência dos sistemas de informação e comunicação, a partir de então o ciberespaço passou a compor, de fato, a agenda estatal. Em um esforço coordenado entre Estado,

[5] A resiliência cibernética diz respeito a capacidade de prevenir, reagir e se recuperar de um ataque cibernético.
[6] O orçamento estimado da LPM 2024-2030 é de 413 milhões de euros, desse montante 4 milhões estão previstos para o domínio cibernético.

profissionais do setor digital, responsáveis, públicos e privados, e cidadãos (RÉPUBLIQUE FRANÇAISE, 2015).

De maneira análoga, em 2017, foi lançada, pelo Ministério das Relações Exteriores, a *Strategie Internationale de la France pour le Numérique*, apoiada em três pilares: governança, economia e segurança. O contexto global competitivo tornou imperativo consolidar a presença no ambiente digital e estabelecer uma rota de ações para o país, na qual destacou-se a busca por um espaço livre, aberto, democrático, representativo e inclusivo (MINISTERE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES, 2017).

No entanto, a intensidade e a sofisticação das ameaças digitais fizeram com que o Estado francês necessitasse mobilizar capacidades e competências diversas, de forma a preservar os interesses nacionais. Em vista disso, foi publicada, em 2018, a *Revue stratégique de cyberdéfense*, a qual pretendia delinear uma estratégia mais robusta e que melhor integrasse os meios para a defesa cibernética[7] (RÉPUBLIQUE FRANÇAISE, 2018).

O primeiro objetivo traçado na Revisão, também conhecida como o Livro Branco da Defesa Cibernética, foi encrudescer os dispositivos disponíveis de proteção cibernética e reforçar a resiliência das redes estatais e de operadores de serviços essenciais, garantindo o seu fornecimento contínuo. No âmbito internacional, a ação da França deveria buscar a regulamentação do ciberespaço, via direito internacional, a prevenção dos ataques, por meio do reforço da cooperação técnica e uma maior capacitação para o gerenciamento de crises (RÉPUBLIQUE FRANÇAISE, 2018, MOLNÁR, 2019).

Do mesmo modo, a Revisão elencou sete princípios da defesa cibernética: priorizar a proteção dos sistemas de informação, adotar uma postura ativa de desencorajar ataques, exercer plenamente a soberania digital, conferir responsabilidade penal aos cibercriminosos, promover uma cultura compartilhada de segurança digital, contribuir para uma Europa mais confiante e segura digitalmente e atuar no âmbito internacional em prol de uma governança coletiva do ciberespaço. Nesta esteira, apontou seis missões: prevenção, antecipação, proteção, detecção, atribuição e reação (remediação, repressão das infrações e ações militares) (RÉPUBLIQUE FRANÇAISE, 2018, p. 9).

Dedicou, ainda, algumas páginas aos aspectos legais que envolvem as capacidades cibernéticas, bem como os riscos políticos, judiciais e militares do seu uso ofensivo. O documento enfatizou a necessidade de as lideranças políticas estarem cientes dos possíveis impactos ao decidir utilizá-las (DELEURE, DESFORGES, GÉRY, 2019)

[7] Antes disso o documento prospectivo e estratégico Action Terrestre Future, de 2016, havia considerado o ambiente digital como um espaço para ação, capaz de multiplicar a eficácia das ações militares clássicas (PROSPERI, 2021, ÉTAT-MAJOR DE L'ARMÉE DE TERRE, 2016).

Por fim, o documento concluiu com uma lista de cerca de cinquenta recomendações, todas elas com prazos para implementação (imediato, curto, médio ou longo) especificados. Destaca-se, por exemplo, a urgência em se definir uma doutrina de ação face a um ataque cibernético, o que requer a criação de um esquema de classificação dos ataques e a definição das opções de resposta aos incidentes. E, em médio prazo, a difusão de uma cultura de segurança digital à sociedade, por meio, entre outros, de um aplicativo para celulares (RÉPUBLIQUE FRANÇAISE, 2018).

Isto posto, em 2019, a França assume uma doutrina clara de defesa cibernética, organizada em dois polos: de um lado, a *lutte informatique offensive (LIO)* e, de outro, a *lutte informatique défensive (LID)*. A LIO diz respeito ao conjunto das ações realizadas no ciberespaço que produzem efeitos contra um sistema antagônico, sejam eles materiais (neutralização de um sistema de armas) ou imateriais (obtenção de dados) (MINISTÈRE DES ARMÉES, 2019a).

A LIO pode ser utilizada isoladamente ou combinada com capacidades convencionais, amplificando o seu potencial, em manobras que requerem um planejamento longo e específico. O principal objetivo da LIO é contribuir para a supremacia militar, com a coleta ou extração de dados, redução ou neutralização das capacidades oponentes e modificação da capacidade de análise do adversário, sem, necessariamente, um contato físico com o oponente (MINISTÈRE DES ARMÉES, 2019a).

O uso da LIO é determinada por lei, pelo contexto político e operacional e por uma avaliação de custos e benefícios. Neste contexto, está sujeita aos princípios e regras do direito internacional e aos regulamentos nacionais (MINISTÈRE DES ARMÉES, 2019a).

As principais linhas de ação da LID são, em síntese, a antecipação, a detecção e a reação. Igualmente, contribui com as missões de prevenção, proteção e atribuição e proposição de estratégias de resposta. A LID reúne, portanto, as ações, técnicas e não técnicas, para lidar com um risco, uma ameaça ou um ataque cibernético real (MINISTÈRE DES ARMÉES, 2019b).

Ressalta-se, ainda, a adoção de uma postura de defesa cibernética permanente (24 horas/7 dias na semana) e a definição de uma classificação da intensidade das ameaças, a partir de uma escala de cores (amarelo/vermelho/escarlate) (MINISTÈRE DES ARMÉES, 2019b).

Dois anos mais tarde, em 2021, foi acrescido ao quadro doutrinário dedicado ao ciberespaço o documento *Doctrine Militaire de Lutte Informatique d'Influence* (L2I). A doutrina advém da importância crescente das mídias sociais no cotidiano da população e a noção de que o ambiente informacional onipresente afeta, também, as operações militares e os processos de tomada de decisão, sejam por meio da manipulação das informações ou pela propagação de notícias falsas (MINISTÈRE DES ARMÉES, 2021b).

Assim, as operações L2I consistem, essencialmente, em informar, defender e agir. Podem, por exemplo, detectar ataques na rede de computadores suscetíveis a gerarem prejuízo à reputação

das Forças, coletar informações e realizar operações de dissimulação, induzindo o adversário ao erro (MINISTÈRE DES ARMÉES, 2021b).

Problematiza-se, contudo, conforme a própria Doutrina L2I afirma, a necessidade de promover parcerias “com empresas especializadas no meio digital” (MINISTÈRE DES ARMÉES, 2021b, p.13) para a ação. Desta maneira, o sucesso das operações está, em partes, condicionado a ação voluntária das plataformas de redes sociais, as quais, em sua maioria, não são nacionais e estão, constantemente, sob pressão para o combate à desinformação (THIBOUT, 2022).

4. ORGANIZAÇÃO INSTITUCIONAL

Os documentos estratégicos franceses foram hábeis ao definir a vocação e as responsabilidades de cada uma das instituições com atribuições no ciberespaço (LE GUÉDARD, 2019), o que nos permite mapeá-las nessa seção. Para tanto, é importante recordar o particularismo do modelo francês de resposta aos incidentes digitais, o qual preza pela separação entre as capacidades defensivas das ofensivas.

A estratégia ofensiva francesa é prerrogativa da presidência através do Conselho Nacional de Defesa e Segurança (CDSN), responsável pela produção de diretivas, as quais são implementadas pelo Comitê de Gestão da Defesa Cibernética (CDC), alocando os recursos necessários. É incumbência da Direção Geral de Controle de Armamento-Informação (DGA-MII) a concepção das armas cibernéticas, seja para os serviços de inteligência ou para o COMCYBER (LE GUÉDARD, 2019).

Constituído em 2017, o COMCYBER está diretamente subordinado ao Chefe do Estado-Maior das Forças Armadas, e consiste em um ator fundamental para a organização e padronização da ação ofensiva no domínio cibernético, bem como para o fortalecimento de uma postura proativa do país nesse ambiente (GERY, 2020). Sua existência equipara o ciberespaço aos domínios terrestre, aéreo, marítimo e espacial (PROSPERI, 2021).

Conforme o artigo D. 3121-14-1, o COMCYBER é o comando responsável pelas ações ofensivas e defensivas. Está no centro da detecção dos ataques e contribui, por meio do compartilhamento de informação, para uma boa compreensão das ameaças.

Em sua estrutura operacional estão, também, os centros operacionais de segurança (SOC), encarregados da supervisão dos sistemas e o centro de análise (CALID), o qual fornece uma visão técnica geral, o Centro de Auditorias de Segurança de Sistemas de Informação (CASSI) e o Centro de Preparação Operacional de Reserva e Defesa Cibernética (CPROC). No topo do arranjo, para orientar a atividades dos demais centros, está o centro de operações cibernéticas (CO Cyber).

Por sua vez, a estratégia defensiva é de prerrogativa do Primeiro-Ministro, através do Comitê Diretor de Cibersegurança (CPC), presidido pela Agência Nacional de Segurança de Sistemas de Informação (ANSSI), instituída pelo decreto nº 2009-834 de 7 de julho de 2009.

A ANSSI é a autoridade nacional responsável pela segurança dos sistemas de informação, com poder regulador, para definir regras de certificação e qualificação de produtos e serviços e de imposição de medidas nos casos de condutas criminosas.

Ao chefe geral da ANSSI é confiado, pelo primeiro-ministro, a responsabilidade de conduzir as operações de proteção e garantir a segurança nacional em caso de um ciberataque. Sob a autoridade do presidente da república, o chefe das Forças Armadas fica encarregado pelas ações militares e de defesa nacional.

Dirigido pela ANSSI, o Centro de Coordenação de Crise Cibernética (C4) é um órgão interministerial de análise de ameaças e troca de informação. Reúne, além da ANSSI, a *Direction Générale de la Securité Extérieure* (DGSE), a *Direction Générale de la Securité Intérieure* (DGSI) e o *Commandement de la Cyberdéfense* (COMCYBER).

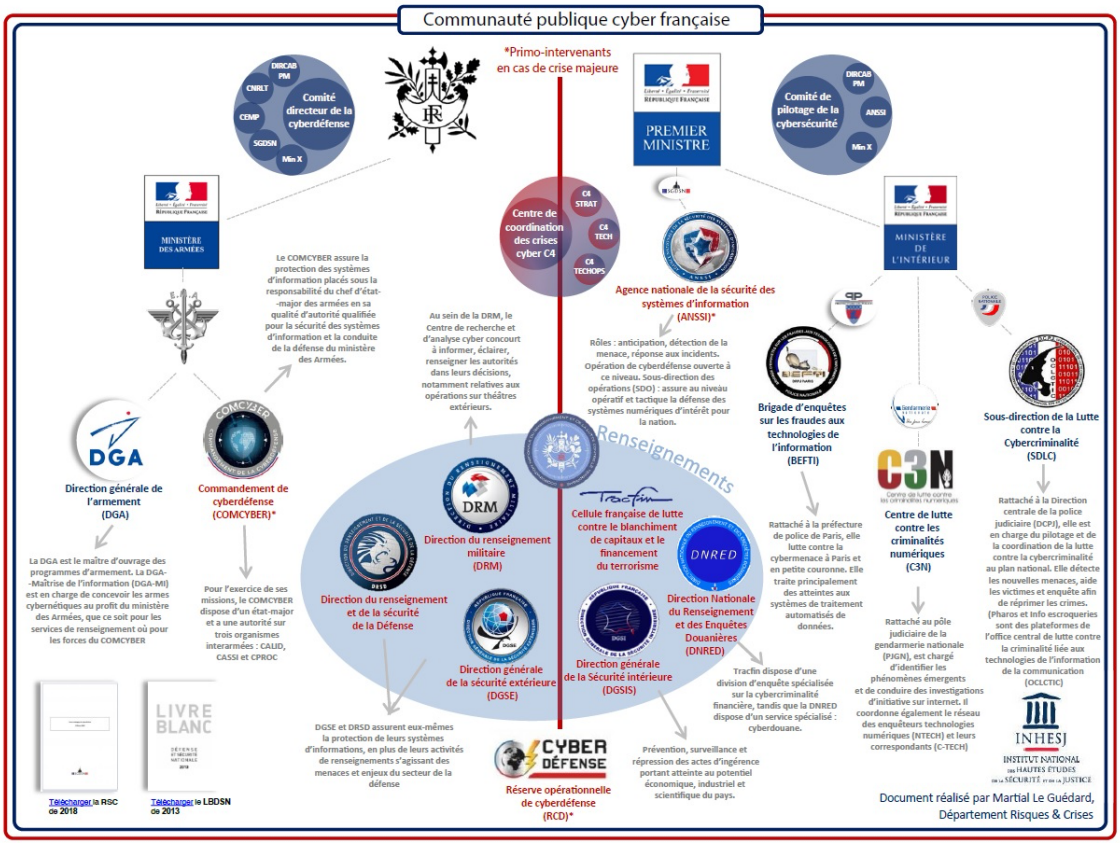
A existência do C4 denota a importância dos intercâmbios e do apoio interministerial em caso de ataque, além de facilitar a resposta operacional, nomeadamente através do C4 TECH, que garante a troca de informação e o diálogo entre os atores (LE GUÉDARD, 2019).

A DGSE e a DGSI tratam o ciberespaço no quadro geral de suas atribuições. A DGSE recruta especialistas para atuarem na identificação e antecipação das ameaças contra a nação, em atividades como: vigilância, interceptações e penetrações de redes de computadores estrangeiras. A DGSI, por sua vez, é responsável por ameaças relacionadas a espionagem, terrorismo, subversão violenta e econômica. As Direções possuem a ferramenta técnica e atuam em apoio às operações militares (VIDELIN, 2018).

No que tange ao combate ao cibercrime é, principalmente, de responsabilidade do Ministério do Interior e do Ministério da Ação e Contas Públicas. No Ministério do Interior, três instituições atuam diariamente: a Polícia Nacional, através da Subdireção de Combate ao Cibercrime (SDLC), as Brigadas de Investigação de Fraude nas Tecnologias de Informação (BEFTI) e o Departamento Nacional Gendarmerie, através do seu centro de luta contra o crime digital (C3N) (LE GUÉDARD, 2019).

A figura abaixo (Figura 1) apresenta, de modo esquemático, os atores que conformam a comunidade cibernética francesa:

FIGURA 1. MAPEAMENTO INSTITUCIONAL



FONTE: Le Guédard (2019).

Não obstante a distribuição de competências, frisa-se que, ainda assim, existem ligações estreitas entre as organizações responsáveis pelas ações ofensivas e defensivas, como, por exemplo, quando se trata do compartilhamento de conhecimento entre o CALID e a ANSSI (LE GUÉDARD, 2019).

Para mais, a capacidade nacional de projetar e implementar políticas públicas para o setor cibernético é desvelada, também, pela criação de diversas equipes regionais de resposta de emergência (CERT)[8], dedicadas a prevenir, registrar, analisar e tratar os incidentes na Internet, além de contribuir com estudos técnicos e com a manutenção de bancos de dados.

O desenvolvimento contínuo da indústria cibernética francesa é outro aspecto importante. Nesse sentido, o país conta com o Cyber Campus, um ambiente que reúne os principais atores nacionais e internacionais da área, com o intuito de aproximá-los e promover parcerias. Além disso,

[8] CERT-FR, dedicado às autoridades francesas; CERT-DEVOTEAM; Cert-IST dedicado às indústrias, serviços do terceiro setor; CERT LA POSTE; CERT-LEXSI(Cybersecurity Expertise Laboratory); CERT-RENATER; CERT-societegenerale; CERT-XMCO; CSIRT-BNP Paribas; Orange-CERT-CC; CERT-SOLUCOM; CERT Crédit Agricole;; CERT Banque de France; CSIRT Bull; Airbus Group CERT.

há um ecossistema de defesa cibernética na cidade de Rennes, o qual abriga o COMCYBER, laboratórios, estabelecimentos de ensino superior e multinacionais do setor (MOLNÁR, 2019).

Outra iniciativa inovadora do Ministério da Defesa, em colaboração com a gendarmeria francesa, é a Rede de defesa Cibernética da Reserva Cidadã (RCC), que se trata de um contingente da reserva especializado na área, composto por voluntários com notória expertise e interesse em questões de defesa nacional. A RCC é, acima de tudo, um importante vetor de ligação entre a sociedade civil e a sociedade a militar, além de um instrumento para sensibilização da população da importância do domínio cibernético (MOLNÁR, 2019).

Finalmente, a França atribui grande importância às relações bilaterais, dentre elas a relação celebrada com a Alemanha, com quem tem desenvolvido uma política de segurança cibernética[9], além da relação com a Índia e o Reino Unido, na qual se tem celebrado diálogos em que são apresentados os últimos avanços em suas respectivas políticas para o setor, identificadas potenciais áreas para aprofundar parcerias, assim como são coordenados esforços[10] para garantir um ciberespaço livre, aberto, inclusivo e seguro.

Outrossim, a França é ativa nas discussões da Organização das Nações Unidas (ONU) sobre comportamento responsivo no ciberespaço, além de participar na Aliança Atlântica, no grupo *Ise-Shima* Cyber e na Organização para a Segurança e Cooperação na Europa (OSCE), entre outros grupos que possuem a cibernética em sua agenda. A prática está em consonância com enunciado pela política internacional francesa, a qual preza pela diplomacia (MOLNÁR, 2019).

5. CONSIDERAÇÕES FINAIS

O modelo de governança francês do ciberespaço é resultado de uma reflexão iniciada há vários anos, especialmente desde o Livro Branco de 2008, e se destaca por representar uma tentativa de separar as missões e as capacidades ofensivas das defensiva.

Do ponto de vista da ciência política, a partilha de poder entre burocracias concorrentes e a fragmentação da autoridade suscita em algumas vantagens incontestáveis. A primeira delas, e mais evidente, diz respeito a maior transparência no direcionamento dos investimentos e na alocação de recursos. Mais do que isso, esse modelo permite, por meio da ANSSI, que haja o desenvolvimento de relações de confiança mais sólidas entre os atores privados e os serviços do Estado.

Contudo, distinguir as missões gera críticas inevitáveis. A principal delas no que tange a eficácia, em razão do inconveniente de uma bipolaridade fortemente assumida. Nesse caso, a

[9] *Bundesamt für Sicherheit in der Informationstechnik*

[10] Cita-se, por exemplo, o Programa de ação para promover o comportamento responsável do Estado no uso de tecnologias de informação e comunicação no contexto da segurança internacional, coordenado por França e Reino Unido na ONU.

ANSSI, que não possui prerrogativa ofensiva, ao responder por um ataque que afete a segurança da nação, estaria desviando de suas atribuições precípuas e poderia sofrer julgamentos de terceiros.

À vista disso, a publicação, em 2019, da LIO e da LID, foi fundamental para fornecer instruções mais específicas aos agentes franceses sobre quais são suas permissões, além de distribuir as tarefas, evitando hesitações e debates em momentos em que a ação deve ser rápida e decisiva (DABILA, 2020).

Depreende-se, portanto, que a implementação progressiva de diferentes documentos e doutrinas possibilitou à França, apesar de um contexto orçamentário restrito, consolidar um modelo em que o Executivo e o Estado-Maior atuam em estreita colaboração e de maneira integrada. Outrossim, as medidas adotadas nas últimas décadas fizeram com que a França conquistasse um reconhecido nível de especialização, aliado a um bom nível técnico e operacional no ciberespaço.

Entretanto, em um contexto no qual o ciberespaço e as operações cibernéticas são, cada vez mais, importantes para projeção de poder e garantia da soberania estatal, manter-se entre as nações mais poderosas no ciberespaço exigirá da França e de seus líderes esforços constantes, especialmente financeiros. Nesse sentido, resta claro que o investimento no domínio cibernético e o uso estratégico desse domínio é, sobretudo, um meio para garantir a soberania, a segurança, a defesa, a resiliência e o desenvolvimento nacional (SHELDON, 2013).

* Artigo recebido em 20 de setembro de 2023,
aprovado em 13 de setembro de 2024.

REFERÊNCIAS

DABILA, Antony. **L'Intégration numériquedes armées, de l'incorporation tactique à la conjonction stratégique**. HAL Open Science, IESD, 2020.

DELERUE, François, DESFORGES, Alix, GÉRY, Aude. **A Close Look at France's New Military Cyber Strategy**. War on the Rocks, 2019. Disponível em: https://warontherocks.com/2019/04/a-close-look-at-frances-new-military-cyber-strategy/. Acesso em: jul. 2023.

DELERUE, François, GÉRY, Aude. **The French Strategic Review of Cyber Defense. Italian Institute for International Political Studies**, ISPI, 2018.

ÉTAT-MAJOR DE L'ARMÉE DE TERRE. **Action Terrestre Future**, Paris, 2016.

FILIPPONE, Dominique. **La cyberdéfense au coeur de la loi de programmation militaire 2018**, Le Monde Informatique, 2018. Disponivel em: https://www.lemondeinformatique.fr/actualites/lire-la-cyberdefense-au-coeur-de-la-loi-de-programmation-militaire-2018-70820.html. Acesso em jul. 2023

GERY, Aude. **La stratégie française de cyberdéfense.** BRENNUS 4.0, 2020.

LE GUÉDARD, Martial. **Organisation de l'État français en gestión de crise cybernétique majeure.** IHEMI, 2019. Disponível em: https://www.ihemi.fr/articles/organisation-de-letat-francais-en-gestion-de-crise-cybernetique-majeure Acesso em: ago 2023.

LISBOA, Cícero, OLIVEIRA, Guilherme. **O conceito de dissuasão cibernética: relevância e possibilidades.** OASIS, 35, pp.53-78, 2022.

MANACH, Jean-Marc. **Les priorités du Comcyber: chffre, lutte informatique d'infuence (L2I) et partage de données.** NextInpact, maio 2023. Disponível em: https://www.nextinpact.com/article/71604/les-priorites-comcyber-chiffre-lutte-informatique-dinfluence-l2i-et-partage-donnees. Acesso em: ago 2023.

MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES. **Stratégie Internationale de la France pour le numérique**, 2017.

MINISTÈRE DES ARMÉES. **Doctrine militaire de lutte informatique offensive (LIO)**, COMCYBER, 2019a.

MINISTÈRE DES ARMÉES. **Doctrine militaire de lutte informatique défensive (LID)**, COMCYBER, 2019b.

MINISTÈRE DES ARMÉES. **Actualisation Stratégique 2021**, 2021a.

MINISTÈRE DES ARMÉES. **Éléments Publics de Doctrine Militaire de Lutte Informatique D'Influence (L2I)**, COMCYBER, 2021b.

MOLNÁR, Dora. **La Cybersecurite en France: le pase, le present et l'avenir.** Hadmérnök, v.14, 2019.

PEZARD, Stephanie, SHURKIN, Michael, OCHMANEK, David. **A Strong Ally Stretched Thin**: **an overview of France's Defense Capabilities from a Burdensharing Pespective**. RAND Corporation, Santa Monica, Calif, 2021.

PROSPERI, Laurent. **Cyberdéfense et conflits armés**, Pantheon Sorbonne, 2021. Disponível em: https://laurentprosperi.info/media/bib/doc_VrANJsJ.pdf. Acesso em: ago 2023

RÉPUBLIQUE FRANÇAISE. **Défense et sécurité des systèmes d'infomation: Stratégie de la France**, Agence Nationale de la Secutité des Systémes d'Information, 2011.

RÉPUBLIQUE FRANÇAISE. **Le Livre Blanc: Défense et Sécurité Nationale**, 2008.

RÉPUBLIQUE FRANÇAISE. **Livre Blanc: Défense et Sécurité Nationale**, 2013.

RÉPUBLIQUE FRANÇAISE. **Strategie Nationale pour la Sécurité Numérique**, 2015.

RÉPUBLIQUE FRANÇAISE. **Revue Stratégique de Défense et de Securité Nationale**, 2017.

RÉPUBLIQUE FRANÇAISE. **Revue stratégique de cyberdéfense**, Secrétariat Général de la Défense et de la Sécurité (SGDSN), 2018.

RÉPUBLIQUE FRANÇAISE. **Revue Nationale Stratégique 2022**, 2022.

SHELDON, John. **Deciphering Cyberpower Strategic Purpose in Peace and War**. Strategic Studies Quarterly, 2011.

SHELDON, John B. The rise of cyberpower. In: BAYLIS, John; WIRTZ, James J.; GRAY, Colin S. (Org.). **Strategy in the contemporary world**: **an introduction to Strategic Studies**. 4. ed. Oxford, NY: Oxford University Press, 2013.

SHURKIN, Michael. **French Army Approaches to High Intensity Warfare in the 21st Century.** WavellRoom, 2022. Disponível em: https://wavellroom.com/2022/06/22/french-army-warfare/. Acesso em: jul. 2023

SHURKIN, Michael. **Why the French Army will continue to prioritize quality over mass**. War on the Rocks, 2023. Disponível em: https://warontherocks.com/2023/04/why-the-french-army-will-continue-to-prioritize-quality-over-mass/. Acesso em: jul. 2023.

SIMÃO, Licínia. França Actualisation Stratégique 2021. In: Pedro Seabra (coord.) **Documentos Estratégicos de Segurança e Defesa**. Instituto de Defesa Nacional, nº44, 2021.

THIBOUT, Charles. **La guerre de l'information: la doctrine française de lutte informatique d'influence (L2I).** Analysis, IRIS, 2022. Disponível em: https://www.iris-france.org/168355-la-guerre-de-linformation-la-doctrine-francaise-de-lutte-informatique-dinfluence-l2i/ Acesso em: ago 2023

TOUJOUSE, Bertrand. **French Land Forces chief: How France's army is transforming for the modern era.** Breaking Defense, 2023. Disponível em: https://breakingdefense.com/2023/05/french-army-chief-how-frances-army-is-transforming-for-the-modern-era/ Acesso em: jul. 2023

VIDELIN, Jean-Christophe. **L'Armée française et la cyberguerre. Olivier Gohin, Xavier Latour**. Annuaire du droit de la sécurité et de la défense, v. 3, mare & mare, p.143-155, 2018.