

Cibersegurança: das Preocupações à Ação

Alexandre Caldas

Vicente Freire

Os *Working Papers* do Instituto da Defesa Nacional resultam de investigação residente e associada, promovida pelo Instituto da Defesa Nacional.

Os temas abordados contribuem para o enriquecimento do debate sobre as questões de segurança e defesa nacional e internacional.

FICHA TÉCNICA

Diretor

Vitor Rodrigues Viana

Coordenação Científica

Isabel Ferreira Nunes

Coordenador Editorial

Alexandre Carriço

Núcleo de Edições

António Baranita e Cristina Cardoso

Propriedade, Edição e Design Gráfico

Instituto da Defesa Nacional

Calçada das Necessidades, 5, 1399-017 Lisboa, Portugal

Tel. + (351)213 924 600

Fax: + (351)213 924 658

Email: idn.publicacoes@defesa.pt

<http://www.idn.gov.pt>

ISSN:

ISBN: 978-972-9393-26-6

Apresentação

O presente *working paper* tem por objetivo sensibilizar para a necessidade de adotar urgentemente medidas de cibersegurança a nível nacional, nomeadamente no que respeita à atribuição e definição da liderança do processo, à organização/sistema em que deve assentar a coordenação e implementação e, ainda, quanto à definição de uma estratégia que dê as orientações para as ações a desenvolver. Para o efeito, considera-se relevar os seguintes aspetos centrais:

- Percecionar o enquadramento do ciberespaço como um espaço de potencialidades e simultaneamente um domínio de elevadas preocupações de segurança;
- Sensibilizar para o imperativo de respostas integradas nestas questões;
- Identificar as principais envolventes na implementação de uma estratégia de cibersegurança;
- Elencar preocupações que requerem medidas de ação imediata;
- Realçar a necessidade constante de acompanhamento continuado dos mecanismos a adotar e a necessidade de garantir evolução e agilização nos procedimentos.

1. Enquadramento: das Potencialidades às Necessidades de Segurança

A Sociedade da Informação tem vindo a oferecer um leque alargado de potencialidades, entre as quais realçamos os contributos para as organizações e sua gestão, para as infraestruturas e a cidadania.

Assistimos de facto a grandes “inovações” nos processos de gestão e de governança, resultado de uma maior valorização da informação e dos mecanismos/meios que aceleram a disponibilidade da mesma. Passam a fazer parte do vocabulário quotidiano: a informação propriamente dita, fluxos de informação, sistemas, tecnologias, *data center*, etc. É certo que as infraestruturas tecnológicas e os Sistemas de Informação (SI) influenciam decisivamente a cadeia de valor das organizações e por isso a economia já não os dispensa porque esta “nova” sistematização de conhecimento permite gerar vantagem competitiva sobre potenciais competidores.

Também as chamadas **infraestruturas críticas, privadas ou públicas**, como telecomunicações, banca e finanças, transportes, energia, água, serviços de emergência, assentam cada vez mais em SI e Tecnologias de Informação e Comunicação (TIC), tornando-se deles dependentes. Aliás, as infraestruturas complexas são mais fáceis de gerir com computadores e sistemas operativos, aplicações e protocolos de redes comuns. Por outro lado, geram-se relações de interdependência entre as infraestruturas, potenciando efeitos dominó quando algum

deles sofre falhas ou impactos negativos (sem eletricidade e telecomunicações a maioria dos sistemas ficam inoperacionais).

Num plano da cidadania, a Sociedade de Informação também veio dar pertinentes contributos. Proporciona uma maior visibilidade à liberdade de expressão individual e o apelo aos direitos enquanto cidadãos – blogues e redes sociais, visíveis mesmo em regimes autoritários e fechados – mas também oferece uma maior democratização no acesso e partilha de informação.

A Sociedade da Informação está em todos os setores da nossa vida!

Paralelamente, **a Sociedade de Informação traz novos desafios no que respeita à segurança**. O seu funcionamento em rede aberta, sem delimitação de fronteiras físicas, as relações de dependência e interdependência entre infraestruturas críticas, as vulnerabilidades de cariz tecnológico e a exposição a ações maléficas ou mesmo de menores cuidados de utilização, torna o ciberespaço muito exposto a novas vulnerabilidades e ameaças, algumas de natureza disruptiva. Noutras palavras, se atentarmos que os mecanismos de geração de riqueza e das infraestruturas críticas do Estado apresentam forte dependência relativamente à informação, ficamos conscientes que essas ações maléficas ou fragilidades podem, assim, afetar o bem-estar, a segurança das pessoas e os interesses nacionais.

Paradoxalmente, **a conectividade é o maior problema da segurança**. Nações internet-dependentes têm muito mais a perder quando a rede “deixa de funcionar”. Se os computadores estivessem isolados os problemas de segurança eram muito reduzidos mas, em contraposição, os benefícios da rede, de estar ligado, da conectividade, são demasiados elevados para serem ignorados. A força da internet – acessibilidade, estruturas colaborativas baseadas em protocolos e tecnologias comuns – infelizmente é o que a torna vulnerável a novos ataques e suscetível de danos massivos ou disruptivos. Importa então um balanceamento entre funcionalidade, desempenho e segurança. É impossível otimizar esse equilíbrio para responder a todos os ataques à rede.

No essencial, **as questões/soluções de cibersegurança devem ter o seu ponto de partida no valor da informação, mais do que nos aspetos tecnológicos** que, embora sendo de tratamento obrigatório e não dispensáveis, são subsequentes. Tal releva a pertinência da reflexão e do debate que o tópico deve merecer e que tem em vista a preocupação da salvaguarda da informação nacional vital e essencial, que obviamente representa o interesse nacional.

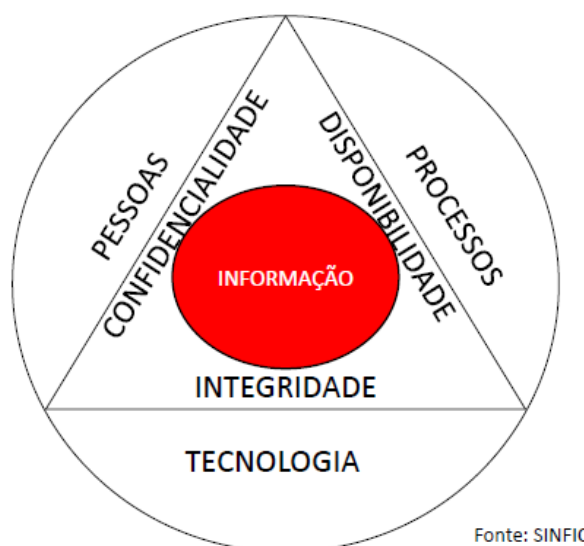
Independentemente de taxonomias mais elaboradas quanto aos objetivos dos ataques estes, maioritariamente, na sua essência, significam perverter a informação, ou melhor, as suas propriedades¹: confidencialidade, integridade e disponibilidade.

A confidencialidade traduz a ideia de evitar uma aquisição não autorizada da informação². A conectividade numa rede global tem facilitado aos *hackers* o roubo de enormes quantidades de informação, mesmo a mais sensível³. A integridade da informação é a garantia de ser a informação verdadeira. Os ataques incluem a sabotagem de dados para propósitos criminosos⁴, políticos⁵ ou militares. O ataque à disponibilidade de computadores ou recursos da informação traduz a privação de utilizadores autorizados acederem aos sistemas para o desempenho das suas tarefas.

Acresce, por outro lado, que da parte dos utilizadores estes querem ter garantido o direito à privacidade da informação que lhe diz respeito.

Tal como se deduz da figura 1, a gestão da informação envolve uma abordagem sistémica, com pessoas, processos e tecnologias.

Figura 1



Fonte: SINIFIC

Atentando a esta realidade, a resolução dos problemas passam nesta sequência para soluções técnicas. Independentemente de considerações mais filosóficas ou conceptuais, nomeadamente sobre tipologias de ataque, os ciberataques estão condicionados ao delimitado terreno do ciberespaço. Embora seja genericamente

¹ De modo mais generalizado são reconhecidas três propriedades. No entanto existem outras, ainda que não consensualmente aceites, a de não repúdio e autenticação.

² Nos ataques à confidencialidade também se inclui a análise de tráfego, em que o atacante infere o conteúdo das comunicações observando padrões de comunicação.

³ A GhostNet, detetada em 2009, era uma rede de ciberespionagem de mais de 1.000 computadores comprometidos em 103 países tendo como alvos a informação política, diplomática, económica e militar.

⁴ Há os que encriptam dados nos computadores das vítimas e depois, por meio de pagamentos, cedem as chaves de descriptação. É um meio de extorsão.

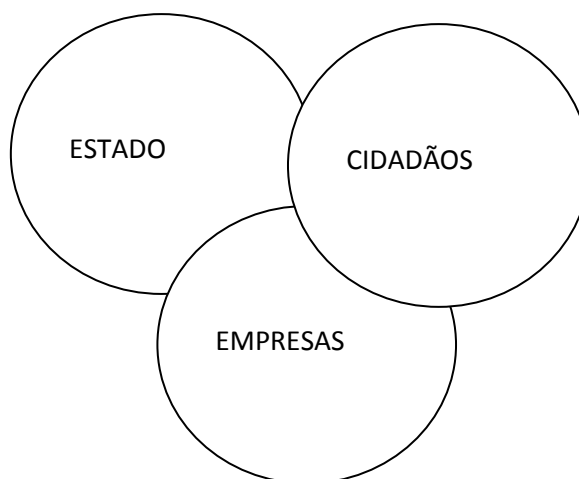
⁵ Países com menor atenção aos direitos humanos editam *e-mails* e inibem os *blogs* dos seus cidadãos.

entendido que a vantagem está mais do lado do atacante do que do defensor, não é totalmente adquirido a garantia do sucesso daquele. Reconfiguração de redes, atualização de *software*, alterações de tomadas de decisão no seio do ciberespaço – padrões de comportamento na rede – são meios e modos que podem desvanecer um ataque. Um defensor tem assim os meios para desenhar e para aumentar o nível de redundância e sobrevivência. Obviamente que dispor de tecnologias de ponta dará vantagem. Tendencialmente muitas das ciberbatalhas serão ganhas por quem usa tecnologias mais recentes.

Claramente poderá ser entendido que **significativa parte das “soluções” são de ordem local porém os desafios colocam-se também a nível estratégico**. A internet evolui a uma velocidade que é impossível para qualquer organização acompanhar todos os últimos desenvolvimentos. Os atacantes têm já subvertido elevado número de sistemas operativos, aplicações e protocolos de comunicação. Os defensores simplesmente têm muito terreno técnico para cobrir, no qual o *hacker* já está em vantagem. Exige-se do defensor criatividade defensiva, boa *intelligence* e algum nível de automação na deteção de ataques e resposta. Aqui o Estado é necessário para dar a sua orientação e contributo.

Em parte, o carácter abrangente do impacto da cibersegurança em sociedade – envolve simultaneamente Estados, cidadãos e empresas – reflete-se no diagrama da figura 2, com a existência de espaços de sobreposição de intervenção dos atores/*players* e outros de alguma autonomia.

Figura 2



Nas sociedades modernas, as áreas de sobreposição de conflito, de sinergias, de dependência e interdependência, necessitam de ser convenientemente identificadas e geridas. O ciberespaço como meio de integração, e sinónimo de sociedades em desenvolvimento, expõe a relevância dos *players* acima identificados e as consequências das suas ações.

Parece-nos pertinente a necessidade dos planeadores nacionais de segurança prepararem as ciberdefesas, quer a nível tático quer estratégico, sem deixar de “exigir” que cidadãos, organizações/empresas e o próprio Estado (a coisa pública) assumam responsabilidades (componente operativa). Por exemplo, a ameaça de ciberataques às infraestruturas críticas, públicas e privadas, é uma questão de índole **estratégica** e requer respostas de igual nível, designadamente: consciencialização do público, investimento em formação, investigação científica, adequada legislação ao ambiente *ciber* e cooperação internacional. A nível da *framework* para enfrentar esta nova realidade, novas entidades – ou talvez apenas algumas mutações nas atribuições das existentes – e coordenação de setores⁶ têm de ser equacionadas. **No caso da proteção das Infraestruturas de Informação Críticas (IIC) não poderão ser só pessoas individuais ou organizações a serem responsabilizadas.** Como sugere o Plano para Proteção de IIC nos EUA (PCCIP) estas são dispositivos coletivos que o governo e o setor privado têm de gerir juntos.

2. O Imperativo de Respostas Integradas

São já inúmeras e sucessivas as ocorrências intrusivas⁷ na internet contra pessoas, organizações/empresas e Estados. O leque varia de ações de espionagem – elevado retorno comparativamente aos métodos de antigamente – a ações de índole criminosa – roubo de identidade, desvios de dinheiro, sabotagem –, de “hactivismo político” a terrorismo, e até mesmo atitudes características de ciberguerra. Para além de *hackers*, criminosos ou terroristas, é reconhecido que há serviços de *Intelligence* de alguns Estados que não se inibem de desencadear ações de espionagem para obtenção e utilização de informação, de modo competitivo ou hostil, para atingir empresas, ou para provocar disfuncionamento/disrupção em IIC ou mesmo perturbação/alteração dos processos críticos de decisão associados ao funcionamento dos Estados.

A amplitude dos ataques, e o tipo de alvos ou objetivos atingidos, premeditadamente, torna claro que as questões de segurança do ciberespaço evoluíram de um contexto iminentemente técnico para um nível estratégico. Não será fruto do acaso que as ciberameaças passaram a constar como uma das prioridades de preocupação no novo Conceito Estratégico da NATO, em 2010.

Por outro lado, o ciberespaço é considerado por diversos países como um novo teatro de operações o qual permite conduzir ações militares⁸ e explorar os recursos disponíveis de forma a exercer coação sobre adversários. Pode afirmar-se que os conflitos políticos e militares têm agora uma ciberdimensão, em que as “batalhas” no ciberespaço podem ser mais importantes do que os eventos que tomam lugar no

⁶ Na opinião do Professor José Tribolet seria uma espécie de um conselho análogo ao Conselho de Chefes Militares (IDN, 21 de setembro de 2011).

⁷ Inclusive com proveniência de Estados.

⁸ Nomeadamente geridas remotamente via internet como é o caso das aeronaves não tripuladas.

terreno, pois são um poderoso meio para uma larga variedade de fins, desde propaganda, espionagem, negação de serviços ou destruição de infraestruturas críticas. O ciberataque não é um fim em si mesmo. A natureza da segurança nacional não tem mudado mas a internet tem providenciado novos mecanismos que podem aumentar a velocidade, a escala e poder de um ataque. A ubiquidade da internet e, simultaneamente, a sua vulnerabilidade, colocam inúmeras ramificações/consequências políticas e militares.

A natureza menos tangível na identificação dos impactos de um mau funcionamento ou interrupção da internet, não significa que não ocorra “sofrimento” – perturbação da energia, perturbação dos transportes. Isto, associado ao facto de não haver efeitos mortais imediatos desses impactos, permite que o poder político esteja atento ao fenómeno mas não se sinta de todo coagido à urgência de medidas. Porém, este é um assunto para a agenda da política e da sociedade sob pena de podermos vir a ser confrontados com o arrependimento por aquilo que se deveria ter feito.

A reflexão torna-se muito pertinente se colocada em termos de qual **a extensão do impacto que os ciberataques têm na segurança nacional**. Nesta perspetiva, o assunto é sério e urgente quando nos situamos em patamares como:

- A fragilidade das infraestruturas críticas dependentes de SI e TIC (genericamente internet) e a sua relevância na vida quotidiana;
- O atrofiamento ou mera afetação da vida económica de uma nação;
- A perturbação dos processos críticos de decisão associados ao funcionamento do Estado;
- O condicionamento do normal funcionamento da vida dos cidadãos, ao nível do seu quotidiano e da sua capacidade de livre expressão.

A Segurança Nacional começa em casa. As preocupações com as ameaças externas ou intrusões vêm depois de nos sentirmos seguros dentro das nossas próprias fronteiras. As ameaças sobre o ciberespaço e as vulnerabilidades deste, em especial sobre infraestruturas críticas e, por conseguinte, vitais na “sobrevivência” enquanto sociedade, exigem das entidades governamentais um constante acompanhamento e adoção de medidas adequadas que importa observar em que moldes estão implementadas.

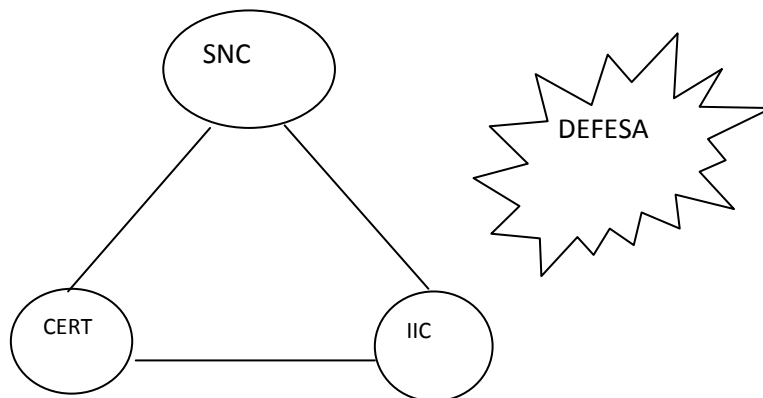
Algumas das principais prioridades são definir, claramente, a quem compete a **liderança** do processo nacional de cibersegurança, a **organização/sistema** em que deve assentar (ou alinhamento estratégico de órgãos) e a definição de uma **estratégia** clara que dê as orientações e nos defina as ações que se irão desenvolver e que se espera ao nível de Estado⁹, organizações/empresas, e mesmo de cidadãos.

⁹ Não só por necessidade mas também porque serve de motor e exemplo para os outros.

3. Eficácia de Atuação: Sinergias e Envolvimento dos “Players”

Segundo a nossa visão, poderíamos “espelhar” a arquitetura do funcionamento da estratégia, numa estrutura triangular, em que a gestão dos problemas do ciberespaço, num modo macro, assenta num sistema – **Sistema Nacional de Cibersegurança (SNC)**¹⁰ – e em áreas de intervenção¹¹: os **Centros de Resposta Rápida a Incidentes Informáticos (CERT/CSIRT)**¹² e as **Infraestruturas de Informação Críticas (IIC)**¹³.

Figura 3



Neste enquadramento, o SNC incorpora a Liderança e Estrutura que dá sustentação ao processo e as questões associadas à informação e sua segurança¹⁴, as políticas. As respostas mais genéricas e de resolução para a defesa no imediato são provenientes dos CERT/CSIRT – rede de CERT sectoriais e um nacional¹⁵. A Defesa (numa perspetiva essencialmente militar) só deve ser interventiva em contexto da sua especificidade (envolvência do Governo e da Presidência da República), não devendo, por isso, estar alheia do que se passa em todo o processo mas estando ligeiramente à parte. As IIC porque são o alvo mais remunerador, sob as quais pendem a estabilidade do

¹⁰ O SNC não se limita a personificar uma entidade ou um qualquer centro mas é antes todo um processo de governança e que incorpora políticas e estruturas.

¹¹ A defesa não é um mero estado de espírito. Requer altos níveis de confiança no *hardware* e no *software*, melhores métricas de desempenho em testes de modelos/cenários de ameaças *hacker*, realizados em laboratório. Nas políticas deverão por isso mesmo estar enquadrados eixos estratégicos que visem uma mais cuidada I&D, ligação às empresas e indústrias do setor da segurança informática e formação de recursos humanos.

¹² Para intervir em gestão de vulnerabilidades, em emergências e mesmo defesa em contextos muito específicos.

¹³ São nevrálgicas porque vitais para a vivência e sobrevivência da sociedade e em geral são o alvo mais remunerador.

¹⁴ Obviamente que estas políticas deverão refletir-se no mundo real onde para além do Estado, estão as empresas, e os cidadãos. Na área dos cidadãos provavelmente poderá ser mais morosa a intervenção do Estado pois misturam-se questões de direito da privacidade com as de segurança e esse é um balanço de gestão sensível.

¹⁵ Na sequência do protocolo que o Gabinete Nacional de Segurança (GNS) assinou com a NATO, em 2011, em termos publicamente desconhecidos, o CERT nacional dará lugar a um Centro de Cibersegurança, que funcionará em moldes ainda não difundidos.

quotidiano deverão ter enquadramento específico¹⁶ quer em respostas, quer em formas de garantir um funcionamento normal mínimo.

Numa descrição de maior detalhe considera-se que um dos passos mais vitais no estabelecimento de medidas de segurança para o ciberespaço é encontrar a **liderança**¹⁷ do processo de cibersegurança. Via auscultação de competências (capacidades) necessárias, observação de atribuições de tarefas análogas ou mesmo através de perceções subjetivas sobre quem naturalmente poderia assumir essas funções, não seria difícil fundamentar uma escolha e, assim, num curto espaço de tempo, encontrar as entidades capazes de liderar o processo – defendemos um conjunto de entidades, embora com uma a liderar este conselho/colégio¹⁸.

Pelo que nos é dado a observar, para os investigadores e pensadores de segurança e defesa e para os responsáveis pelas IIC, é sensível não haver já uma clara definição de quem efetivamente compete a liderança. É-nos claro que dada a natureza teleológica do que está em causa e a elevada probabilidade de disrupção de sistemas vitais, e para assegurar a verdadeira funcionalidade do processo, a liderança tem de estar na proximidade do chefe do Governo, sob risco dos seus efeitos/implementações não se fazerem sentir transversalmente a todos os ministérios.

A estrutura (organização/sistema) deve ter três níveis: **o executivo** (Comité Executivo) que já associamos à liderança, **um conselho**¹⁹ com um conjunto de especialistas, com obrigatoriedade de serem ouvidos, e cujas recomendações seria desejável, em nosso entender, que em parte pudessem ser mandatórias para o nível executivo e o nível das **comunidades de interesse** – os anglo-saxónicos designam de *communities of practice* – com recolha de ideias, de perspetivas de áreas especializadas e também mais próximas dos cidadãos.

Esta estratificação resulta do facto que **qualquer intervenção em matérias do domínio da cibersegurança deve ser abrangente e envolvente**. Abrangente porque independentemente de existir uma liderança (estrutura de cariz mais executivo) deve existir um *board* (de dimensão comedida) de “conselheiros” que contemple os principais atores – representantes do governo, das áreas sectoriais das IIC, dos Serviços de Informações, das Forças Armadas e de Segurança, da área industrial, da academia, do Centro de Resposta a Incidentes, etc.. A característica “envolvente”

¹⁶ Inclusive devem ser previstos instrumentos/mecanismos que salvaguardem determinados *standards* (provavelmente auditorias, certificações, etc...).

¹⁷ De acordo com intervenções *ad hoc* em conferências parece que a liderança virá a ser assumida pelo Gabinete Nacional de Segurança (GNS) conjuntamente com outras entidades. Aliás, no sítio do GNS estão descritas as linhas gerais de uma Estratégia Nacional de Cibersegurança, parecendo que esta entidade se assume como responsável por estas áreas. Nos termos da Resolução do Conselho de Ministros n.º 12/2012, de 7 de fevereiro, a medida 4, que contempla a definição e implementação de uma Estratégia Nacional de Segurança de Informação, será coordenada pelo GNS.

¹⁸ Parece-nos, de acordo com os termos do sítio do GNS, que se prevê a existência de um Conselho de Cibersegurança como uma capacidade de nível estratégico capaz de garantir uma eficaz gestão de crises.

¹⁹ Uma similaridade aos conselhos gerais das universidades.

traduz que se a mensagem não for clara para os atores, no sentido de perceberem que são afetados e que as suas apreensões ou contributos são ouvidos, o processo é desgastante, oneroso e passível de baixos resultados. O estímulo a um fórum de reflexão – por exemplo, o Grupo de Estudos Contributos para uma Estratégia Nacional da Informação (GECENI), do IDN – e a criação de *Think Tanks* poderão ser mais complementos para a procura de soluções. Identificamos esta área como a de Comunidades de Interesse.

A **estratégia**, enquanto elemento aglutinador, é a materialização num plano de ação das orientações, das ações e das prioridades. É extremamente simples traduzi-la em legislação bastando quase “decalcar”, com as devidas adaptações, por uma das estratégias de cibersegurança de entre os 13 países²⁰ que já publicaram as suas. A essência do problema parece-nos estar mais na capacidade de envolvimento da sociedade para esse fim comum e na racionalização de investimentos.

A estratégia, para além de ter de envolver aspetos políticos, o governo deve ter a esse nível uma visão macro dos problemas sem esquecer a objetividade de criar mecanismos para os resolver. Só faz sentido ser implementada se equacionar a solução dos problemas de modo completo e com eficácia. No mundo real, o que verdadeiramente está em causa é a segurança – relativamente a ameaças intencionais e intrusivas – e a confiabilidade – assegurar o funcionamento mesmo contra ameaças e desastres acidentais – de algo materializável: a informação (propriamente dita) e as infraestruturas de informação (sistemas, redes).

Assim, **a estratégia deve dar resposta ao que proteger²¹, ao que valorizar na proteção²², analisar as causas de impedimentos à segurança e confiabilidade e como fazer (procura de soluções).**

Na análise das causas de impedimentos é relevante ir além dos efeitos – daquilo que se vê ou se sente – e refletir/analisar sobre a caracterização das ameaças reais, vulnerabilidades e riscos. O como fazer leva-nos a propostas de *modus operandi*, de nível estratégico ou tático, mas tendo subjacente que deverão estar definidos os objetivos para a mitigação de riscos²³. Complementar e paralelamente a este processo, há que identificar as partes interessadas/envolvidas, quem obtém proteção e quem é chamado a contribuir/agir.

²⁰ Sinónimo da urgência e da relevância que a temática lhes merece são já 13 os países com Estratégias de Cibersegurança, a saber: África do Sul, Alemanha, Austrália, Canadá, Estónia, EUA, França, Holanda, Japão, Nova Zelândia, Reino Unido, República Checa e Polónia.

²¹ O que proteger aponta para os ativos (inclui a informação) segundo uma lógica de criticidade na perspetiva da natureza (digital ou físico, informação ou infraestrutura), de tipificação (público, privado, militar,...) e de impacto geográfico (local, nacional,...).

²² O valor é encarado na cadeia – valor organizacional dentro da própria instituição e na sua (inter)dependência com outras – e em termos operacionais – funcionamento do sistema e por conseguinte confiabilidade técnica.

²³ Pode definir o maior ou menor grau de profundidade de empenhamento.

Independentemente da estratégia que vier a ser adotada há alguns eixos que fazem sentido ser equacionados:

- **Uma visão política que se sobreponha no tempo, significativamente mais do que o período de uma legislatura, desejavelmente dez anos;**
- O reforço de competências especializadas dos recursos humanos, não só de cariz tecnológico mas também das áreas militar, sociologia, psicologia, ciência política e de economia e diplomacia;
- A adoção de modelos de estímulo ao investimento ou de financiamento para o setor privado, em boa parte garante do sucesso da cibersegurança;
- O desenvolvimento de modelos de cooperação nacional e de ação estratégica em rede, nomeadamente áreas sectoriais, forças de segurança e defesa, serviços de informações, academia, etc..
- A mobilização de empresas, universidades, cidadãos para especializações e inovações seletivas, nomeadamente na área da I&D²⁴;
- A monitorização e avaliação não só dos trabalhos desenvolvidos (mecanismos de correção e de potencial cooperação para sinergias) mas também das ameaças e oportunidades;
- O desenvolvimento dos mecanismos que assegurem a cooperação internacional em áreas em que as medidas nacionais não são suficientes e projeção de uma imagem de maturidade nas questões de cibersegurança junto dos parceiros internacionais;
- O acompanhamento e integração das evoluções tecnológicas dos países mais desenvolvidos e em geral da comunidade internacional;
- A promoção de uma maior proximidade dos problemas reais nomeadamente com a definição de um Centro Nacional de Resposta a Incidentes (CERT.PT/CSIRT²⁵), o incentivo ao uso de “boas práticas” e, provavelmente, em determinados setores, a exigência de certificações (ISO 27000);
- A consciencialização da sociedade para as questões de cibersegurança e articulação de uma estratégia de comunicação com recurso aos *media*.

Julgamos que são também **instrumentos de governança**²⁶ e de sustentação, em complemento da estratégia, uma política de proteção da informação, uma política de

²⁴ Áreas seletivas porque têm de existir uma consciência da impossibilidade de atuar em todas as áreas. No que respeita às inovações, Portugal não tem de reear o futuro e os seus riscos, que esse oferece, face às provas de inovação dadas ao longo da sua história.

²⁵ Previsivelmente “personificado” no Centro de Cibersegurança já criado mas não implementado.

²⁶ E também consecução da estratégia

gestão da segurança da informação, um plano/política de resposta a incidentes²⁷ e um plano de proteção de infraestruturas críticas.

Assim, **no domínio do ciberespaço, para que uma estratégia possa ser implementada com sucesso é importante saber que informação proteger e por isso dispor de um plano de proteção da informação.** A nível do Estado, importa identificar o que é a “informação nacional”, onde ela anda, quais as entidades informacionais e os recursos existentes. Um recente trabalho desenvolvido por um grupo coordenado por um assessor do primeiro-ministro, parece indiciar estarem a ser dados passos relevantes quanto à integração e centralização de sistemas e na identificação dos recursos disponíveis. Há porém, em nosso entender, uma cultura que tem ser adquirida no Estado em dois particulares aspetos: a necessidade de observabilidade e controlabilidade da informação – quem a usa e as rotas/fluxos dessa informação de forma a assegurar que não está nas mãos erradas²⁸ – e implementar uma boa prática, típica das grandes empresas, de separar os *e-mails*/conteúdos pessoais dos funcionários públicos daquilo que é do Estado²⁹.

Numa política de Gestão de Segurança da Informação deve-se enquadrar aspetos de índole mais técnica e definir um plano de ação com metas que possam ser devidamente avaliadas e monitorizadas. Assegurar as propriedades da informação (confidencialidade, integridade, disponibilidade) passa por mecanismos de prevenção, deteção e mitigação de riscos. Não pode, porém, ser esquecido que a montante deve proceder-se ao levantamento de vulnerabilidades e ameaças³⁰ nos Serviços de Informações.

Para uma política de Resposta a Incidentes (ciberataques), os quais já tendem a ser em elevado número, não pode apenas continuar a ser vista uma postura reativa³¹ pela parte dos CERT/CSIRT. Poder-se-á exigir respostas de outro nível, diplomáticas ou militares ou meramente intervenções pró-ativas.

Um plano de proteção de infraestruturas críticas terá também de existir³² porque elas são vitais à sobrevivência e ao bem-estar das populações e, infelizmente, têm sido

²⁷ A realizar pelo CERT.pt. A sua alocação tem tido diferentes soluções nos países onde estão já implementados. Em Portugal não está alocado mas não é muito difícil escolher a sua atribuição. Porém, alerta-se que um modelo exclusivamente militar não faz sentido, bem como ser exclusivo das academias, ou das telecomunicações ou dos serviços de informações, etc... Tem que integrar vários setores.

²⁸ Não é controlo de privacidade dos utentes mas do uso da informação sensível.

²⁹ Referimo-nos aos computadores da Administração Pública.

³⁰ Recolha e análise a partir dos serviços de informações (elemento vital no processo) e também a partir dos dados provenientes dos relatórios do CERT.

³¹ Maioritariamente, talvez até seja só uma partilha de “dores de cabeça” com situações vividas e a difusão das lições aprendidas.

³² Em Portugal, já há algum trabalho feito como adiante se refere.

alvo de algumas intrusões³³, não fruto do acaso. Nesse plano devem ficar claras questões como:

- O que é uma infraestrutura crítica (ou talvez porque o é)?
- Se está conectada à internet/rede?
- Se é dependente das tecnologias de informação (TI)?
- Se a sua perda é uma ameaça à segurança nacional?
- E no caso de falhar se é recuperável?

Complementarmente, o papel dos *media* para reforçar a postura de segurança para com o ciberespaço constitui-se de enorme relevância para a consciencialização de toda a sociedade, não só para os problemas existentes mas, também, para a sensibilização de que se vive realidades diferentes das que estávamos habituados no passado.

A intervenção de cariz **política, a uma escala global**³⁴, passará talvez, como sugere Keneth Geers³⁵, por quatro abordagens³⁶ na postura de um Estado/Nação em termos de cibersegurança, como resposta de mitigação aos ciberataques:

- (1) A adoção do *Internet Protocol version 6* (IPv6).
- (2) A doutrina militar³⁷, muito subjacente à *Arte da Guerra*, de Sun Tzu.
- (3) Dissuasão dos ciberataques.
- (4) Controlo de ciberarmas.

O IPv6³⁸ é uma solução técnica de escala global. A doutrina militar é uma solução militar. A dissuasão é uma mistura de considerações políticas e militares. O controlo de

³³ O presidente Obama, dos EUA, em maio 2009, referia que ciberataques tinham deixado cidades inteiras na escuridão. Referia-se provavelmente aos apagões de 2005 e 2007 no Brasil.

³⁴ Hoje, os ciberataques podem atingir lideranças políticas, sistemas militares, cidadãos anónimos (figuras não públicas) em qualquer parte do mundo, em tempo de paz ou de guerra, sob o benefício de tal ser feito sob anonimato. Acresce que a ciberdefesa é um processo infindo e as investigações de ciberataque são tipicamente inconclusivas. Por isso, a nível dos líderes militares, visível nos EUA, está-se unicamente a procurar deixar para trás conceitos sobre defesas cibertáticas e reativas para formular políticas estratégicas e proactivas. Cf. Kenneth Geers, 2011, *Strategic Cyber Security*, p. 113.

³⁵ Num trabalho intitulado *Strategic Cyber Security*, 2011, de Kenneth Geers, disponível em www.ccdcoe.org/278.html, CCDCoE, onde as abordagens são bem refletidas pese embora tenha como enquadramento os EUA.

³⁶ Das quatro apresentadas, as duas últimas estão em processo de gestão/amadurecimento.

³⁷ Os exemplos de ciberataques já ocorridos no mundo real sugerem que a ciberguerra jogará, no futuro, um papel relevante nos conflitos internacionais.

³⁸ O IPv6, só por si, não é sinónimo de resolução eficaz. De facto, a captação de endereços IP nesta tecnologia torna-se um maior pesadelo para os intrusos e a facilidade com que se escondem no anonimato diminui significativamente pela maior dificuldade de encontrar os IP (alvos). Todavia, a análise de tráfego, que é possível no IPv6 vai também permitir identificar conteúdos, e, assim, os objetivos dos intrusos poderão ser obtidos por outra via, ainda que com maior dificuldade. Por outro lado, a sobreposição por mais largos anos com o protocolo antecessor, IPv4 (substituição total é um grande investimento) permite a exposição de fragilidades de ambos os sistemas. Mesmo quando o IPv6 for único, não é garantida total segurança mas apenas uma maior eficácia.

ciberarmas é uma solução política/técnica. As soluções técnicas e militares são relativamente entendíveis pelo que se detalhará um pouco mais o enquadramento da dissuasão³⁹ do ciberataque e controlo de ciberarmas.

A dissuasão proposta por Keneth Geers prevê duas metodologias: a negação de aquisição de tecnologias ameaçantes e a punição. O autor procede a essa análise sob as perspetivas de capacidade, credibilidade e da comunicação/visibilidade. Considerando dois aspetos desafiantes ao nível de ciberataques, que são a atribuição dos ataques e a sua assimetria, infere que a dissuasão é uma tarefa praticamente impossível. Por exemplo, o principal desafio da anti-proliferação é definir o código comprometido, porque podem ser usados caminhos legítimos para roubar segredos nacionais. Mesmo para os especialistas poderá ser tarefa “exigente” identificar o “erro” no meio da análise de um elevado número de linhas de código. Assim, proibir o desenvolvimento de ciberataques via Tratados Internacionais pode até banir iniciativas de ataque e de disrupção de redes não combatentes mas aumenta a gestão internacional da internet (se é que existe) e pouco melhora no problema essencial, a questão das atribuições.

No que respeita à dissuasão com recurso à punição esta tem de ser entendida como último recurso, e só depois de esgotados os instrumentos da negação. A punição tem como objetivo a prevenção da agressão com a ameaça de uma maior agressão, tida como dolorosa ou de retaliação. Isso significa que o agressor tem de ficar convencido que a vitória não é possível. Novamente, os aspetos da atribuição e da assimetria estão em causa. Na parte relativa à atribuição, a capacidade de responder está posta em causa⁴⁰ por dificuldade da sua identificação. No respeitante à assimetria está comprometida a credibilidade com a desproporção dos meios.

A quarta abordagem, relativa ao controlo de ciberarmas corresponde à tentativa de adotar a filosofia vigente na Convenção para Armas Químicas uma vez que, a nível da comunidade internacional, esta tem garantido algum êxito. Assim, seria a adoção de algo como um Tratado Internacional de Controlo de Ciberarmas. Há algumas características que são apontadas a tratados desta natureza: a vontade política, a universalidade (a aplicação global), a assistência (ajudar os signatários), a proibição (delimitação) e inspeção (a possibilidade de qualquer signatário ser observado sem aviso prévio e em qualquer lugar). As três primeiras características ainda se podem aplicar a ciberarmas, pese embora a vontade política possa ser a mais difícil. No que respeita à proibição e à inspeção, afigura-se serem características não plausíveis de

³⁹ É relevante lembrar que a Teoria da Dissuasão emergiu na sequência de os EUA e a URSS terem criado “poderio” militar suficiente para destruir a civilização humana no planeta. Para o estrategista Bernard Brodie, 1946, essa teoria significa ganhar as guerras pela prevenção em relação a elas. Os *hackers* podem roubar tecnologia de armas ofensivas (inclui as de destruição maciça) ou fazer render uma inoperável defesa adversária durante um ataque convencional. À luz disto tentar proactivamente deter um ciberataque pode vir a tornar-se uma parte essencial das estratégias militares.

⁴⁰ Inclusive o verdadeiro atacante poderá sempre dizer que o seu computador foi pirateado e usado por alguém.

aplicação ao ciberespaço. A proibição exige o acesso a informação que identifica pessoalmente quem foi o provocador e, por outro lado, exige organização da lei para que possa ser notificado, o que é difícil. Na parte da inspeção há excessiva informação para analisar e o *malware* pode ser transmitido para a rede a partir de qualquer computador (que não o do *hacker*). Em suma, é difícil proibir e inspecionar algo que não se consegue definir e que cresce com uma magnitude elevada. Talvez, como sugeriu o autor, se pudesse começar por objetivos menos ambiciosos e chamar-lhe Convenção de Segurança da Internet.

4. Preocupações no Curto Prazo que Requerem Adoção Imediata

Urge implementar uma **estratégia de cibersegurança** por cinco razões fundamentais:

- A vulnerabilidade de IIC nacionais vitais à sociedade e as ameaças latentes de ciberataques exige um enquadramento global para respostas ao problema;
- É necessário consciencializar cidadãos, empresas e o próprio Estado da nova realidade que o ciberespaço trouxe à sociedade, em termos de alteração de comportamentos e de preocupações de segurança;
- As medidas não podem ser *ad hoc* e deve ficar claro que as potenciais vítimas devem ser os intervenientes no processo de solução e de acompanhamento dos problemas;
- É necessário definir uma política da informação: o que é? Onde está? Por onde anda?;
- É muito pertinente a necessidade de uma Política/Plano de Proteção das Infraestruturas Críticas (PPIIC) dependentes da internet ou das TI.

Associada a uma estratégia há a **liderança** não só da mesma mas também do arranque e instalação de um “Sistema Nacional de Cibersegurança” para garantir a “perenidade” da sustentação da eficácia dos objetivos a que se propõe. A liderança, conforme já referido, poderá ser constituída por três grandes componentes: a Executiva, o Conselho/Consultiva e a Comunidade de Interessados (fórum). A Executiva é um comité executivo (diretor) de atores chave. Deve existir uma entidade líder, na qual deverá residir o secretariado executivo, mas as decisões deverão ser tomadas em colégio. O Conselho/Consultiva, com uma visão orientada para o operacional, a quem compete fazer recomendações, deve assentar numa comissão limitada, em termos de número, constituída por especialistas, devendo os seus membros ser provenientes, sobretudo, de setores-chave, áreas técnicas, académicas e da segurança e defesa. O fórum, deve constituir-se como uma plataforma de diálogo, entre a comunidade de interessados, representativa dos mais variados setores, e ter capacidade de reportar reflexões e preocupações não somente à parte executiva mas também, por via da documentação a um organismo governamental.

Parte significativa da solução dos problemas, pelo menos numa perspetiva técnica, passa na maioria dos países por um **Centro de Resposta a Incidentes em Computadores (CERT/CSIRT)**. Infelizmente, na quase totalidade deles tem mais uma atuação de *helpdesk* (gestão de vulnerabilidades) do que de gestão de riscos (prevenção, deteção, resposta a problemas). Em Portugal, é urgente transformar o CERT.PT, do atual cariz académico para uma abrangência nacional, envolvendo representantes de vários setores e alocá-lo a uma entidade. Uma solução⁴¹, seria, preferencialmente, próximo do setor das telecomunicações ou em áreas de segurança e defesa, por exemplo, em órgãos como o Gabinete Nacional de Segurança (GNS), o Secretário-Geral do Sistema de Segurança Interna (SGSSI), o Estado-Maior General das Forças Armadas (EMGFA)⁴² ou os Serviços de Informações da República Portuguesa (SIRP)⁴³. Seria, no entanto, relevante acrescentar às suas competências, intervenções de cariz mais operacional, ou seja, resposta a ataques num contexto problema/solução e não político.

No imediato, é pertinente dinamizar e acelerar os trabalhos do ex-CNPCE (agora residentes na ANPC) para a conclusão e implementação do **Programa Nacional de Proteção de Infraestruturas Críticas (PNPIC)**⁴⁴, em especial os que estavam associados à Comissão de Planeamento de Emergência do Ciberespaço (CPECIB). Esse programa pretende criar uma base de dados georreferenciada e constituir-se como um “instrumento estratégico fundamental orientador de prioridades de proteção em relação às infraestruturas vitais cuja destruição ou utilização indevida possa afetar significativamente os pilares do funcionamento do País e o bem-estar da sua população”. Em termos concretos pretende: a “classificação objetiva da criticidade de cada infraestrutura crítica; a avaliação de interdependências não só funcionais, como económicas, sociais e temporais; a quantificação e modelação de vulnerabilidades e de consequências face às ameaças plausíveis de afetarem as infraestruturas”. Uma resultante final será a “definição de prioridades na canalização de esforços e recursos para proteção e aumento da resiliência das infraestruturas críticas”.

O PNPIC implementado acaba por traduzir-se no conjunto das três fases distintas a prosseguir com vista ao desenvolvimento do processo da proteção, e que são: (i) identificação e classificação das Infraestruturas Críticas Nacionais; (ii) estudo e difusão

⁴¹ Terá de ser sempre da iniciativa do governo embora o atual CERT.PT tenha tido o seu início no âmbito “privado”. Parece-nos que em sua substituição é criado o Centro de Cibersegurança que segundo fontes do gabinete do primeiro-ministro será alocado à Polícia Judiciária.

⁴² Nos EUA existe um CERT nacional e também um Centro de Ciberdefesa. Este último está alocado num Comando Militar para o Ciberespaço, localizado nas instalações da National Security Agency (NSA).

⁴³ No Reino Unido, o Centro de Operações de Cibersegurança está na dependência dos Serviços de Informações.

⁴⁴ Iniciado por deliberação de um Conselho de Ministros, em 2004, e que atribuiu ao CNPCE, o Projeto Proteção de Infraestruturas Críticas, então chamado “Carta Nacional de Pontos Sensíveis”. A Diretiva Europeia n.º 2008/114/EC de 08DEZ2008, “Identificação e Designação de Infraestruturas Críticas Europeias e sobre a avaliação da necessidade de as proteger”, elaborada pela Comissão Europeia no âmbito do Programa Europeu para a Proteção de Infraestruturas Críticas Europeias (PEPIC), em cuja elaboração Portugal teve uma participação ativa, veio reforçar a iniciativa.

de medidas eficientes para reforço da sua proteção; (iii) implementação de medidas e monitorização do risco. Parece concluída a 1.ª fase e atualmente procura-se o financiamento externo para a segunda. Mesmo num período de crise, como o que atualmente se vive em Portugal, importa efetuar um exercício de prioridades face às vulnerabilidades e à relevância da “sobrevivência” das infraestruturas críticas no quotidiano.

Criar e articular uma **estratégia de comunicação** para a consciencialização da sociedade (Estado, empresas, cidadãos) sobre as questões associadas à segurança na utilização do ciberespaço, poderá passar pela constituição de uma comissão que garanta o encontro de representantes de intervenientes chave, refletindo-se os resultados na educação, na informação e na partilha. Se não se criarem mecanismos para a envolvimento e empatia com os *players* principais e com os cidadãos, uma qualquer estratégia de cibersegurança poderá permanecer muito tempo apenas na letra do papel ou com resultados muito diminutos.

Deverá refletir-se a prioridade e a relevância deste assunto no interesse nacional e **alocar verbas ajustadas** para o efeito como veículo para o investimento, para o estímulo de dinâmicas na área do ciberespaço, envolvendo não somente os potenciais afetados (Estado e IIC), mas também a I&D nas universidades e a indústria nacional no setor. Há potencial de retorno do investimento a nível nacional e de criação de *clusters* de excelência no mercado internacional. Portugal ao longo da história foi pioneiro em muitas inovações: são várias as *start-ups* portuguesas que “vingaram” em Silicon Valley e o mercado da CPLP e da América Latina é muito promissor.

5. Agilização: Controlo, Monitorização e Evolução

Portugal está “muito frágil” em medidas de cibersegurança numa perspetiva de resposta liderada, estruturada e sujeita a entidades organizacionais. Paradoxalmente, há muitas iniciativas de cidadãos e de empresas e de alguns setores do Estado que merecem referência como boas práticas.

Neste contexto, a estratégia de cibersegurança não pode *per se* ser entendida como uma solução redentora exclusiva, para Portugal, mas como uma **abordagem top-down** que enquadra os direitos e deveres, e que, simultaneamente, dinamiza a sociedade para uma finalidade. Por outro lado, há que saber enquadrar na estratégia ou na liderança dela o valor das iniciativas já ocorridas e alimentar uma **abordagem bottom-up** – dos afetados até à intervenção do Estado – para que ambas as abordagens se encontrem no esforço de atingir a finalidade última, proteger o ciberespaço, mobilizando sinergias que evitem redundância de esforços e que atenuem, pelo menos, a vulgar tendência portuguesa de considerar “que o que já foi feito está mal”.

O Fórum de Reflexão (Comunidades de Interesse) afirma-se como elemento de rejuvenescimento e de “**tanque**” de ideias porque é muito lato na abrangência de

sensibilidades e permite auscultar sobre a emergência de novas problemáticas, possibilitando olhar para o hoje e para o futuro com maior serenidade porque “antecipa” novas realidades. Algumas realidades em que fará sentido ter alguma proatividade, antes que sejamos confrontados com evidências serão, entre outras: a “alteração de comportamentos sociais” com os nativos digitais, uma nova postura da comunicação, o papel dos *media* e a projeção da expressão das opiniões de cidadãos anónimos e, ainda, o lugar e o papel da diplomacia na realidade cibernética.

É pertinente a **monitorização periódica do processo de consciencialização** sobre as questões de cibernética através de *surveys* a IIC, a quadros seniores do Estado e a amostras de cidadãos – ter nomeadamente em conta as camadas mais jovens e estudantis.

É relevante ter capacidade de **desenvolver a cooperação internacional** não só nas organizações onde Portugal tem assento (ENISA, Convenção do Cibercrime no Conselho da Europa, ONU, NATO, etc.) mas também em atividades em rede. Tal significa, também, a possibilidade do Estado absorver os *inputs* das mesmas e fazê-los refletir em “território nacional” bem como encontrar os “veículos” para “exportar” as suas ideias e fazer “vincar” as posições e interesses nacionais.

Deverão ser criados mecanismos independentes para **avaliação e monitorização da estratégia de cibersegurança**, do alinhamento das entidades para esse fim e do impacto que as suas ações têm nas estruturas para decidir sobre o que manter, alterar e introduzir por novas ações. As medidas de segurança para o ciberespaço exigem intervenções e comportamentos proactivos e criativos, não só porque os “atacantes” estão em vantagem relativamente aos defensores – “jogar” em casa já não é uma vantagem – mas também porque os *hackers* são “gente” dotada de capacidades intelectuais acima da média.