# REFLEXÕES DAS TÁTICAS NAVAIS: As *clock decisions* no contexto das operações cibernéticas

FLÁVIO DE **QUEIROZ** GUIMARÃES*
Capitão de Mar e Guerra

**SUMÁRIO**



## INTRODUÇÃO

O Almirante Horatio Nelson (1758-1805), o mais proeminente comandante da história naval britânica, conhecido por sua liderança, sua perspicácia estratégica e suas táticas navais inovadoras para a época, teve uma carreira marcada por inúmeras vitórias navais decisivas durante as Guerras Napoleônicas, contribuindo significativamente para a supremacia naval da Grã-Bretanha [1]. A frase do Almirante Horatio Nelson "Time is everything; five minutes make the difference between victory and defeat", ou "O tempo é tudo; cinco minutos fazem a diferença entre a vitória e a derrota" (tradução livre), ressoa profundamente na guerra cibernética, destacando a importância crítica da velocidade na defesa e na resposta às ameaças cibernéticas.

*Mestre em Computação pela Universidade Federal Fluminense (UFF). Especialista em Guerra Cibernética pelo Centro de Instrução de Guerra Eletrônica do Exército (CIGE) e em Política e Estratégia Cibernéticas pela Escola Superior de Guerra (ESG). MBA em Cibersegurança pelo Instituto Brasileiro de Mercado de Capitais (Ibmec) e certificado internacionalmente em Threat Intelligence, Threat Hunting, Threat Modeling, Cyber Risk, Cyber Crisis e Malware Analysis.

## O TEMPO É TUDO

No contexto da guerra cibernética [2], o conceito de tempo não é apenas um componente tático; é a pedra angular estratégica que pode ditar o impacto dos incidentes de segurança cibernética. As ações ofensivas neste domínio da guerra muitas vezes acontecem a uma velocidade alarmante, com *malwares* (código arbitrário que provê uma vantagem para o adversário) se espalhando pelas redes, comprometendo sistemas em minutos, ou mesmo em segundos. A rápida escalada de ataques de *ransomware* (bloqueio de ativos informacionais em troca de resgate para obtenção de vantagem financeira), por exemplo, pode levar à criptografia generalizada dos sistemas operacionais ou de dados, causando interrupções operacionais significativas quase que instantaneamente [3].

**Nos cenários de guerra cibernética, a capacidade de detectar, responder e mitigar ameaças de forma decisiva é crucial**

Nesses cenários, a capacidade de detectar, responder e mitigar ameaças de forma decisiva é crucial. Esta analogia com a observação de Nelson destaca vários aspectos-chave da guerra cibernética:

– Detecção Rápida: a detecção inicial de uma intrusão cibernética é semelhante a avistar o inimigo no horizonte na guerra naval. Quanto mais rápido um adversário for detectado, mais tempo os defensores terão para reunir seus recursos e conter o ataque. Ferramentas automatizadas e monitoramento contínuo são essenciais para alcançar as rápidas velocidades de detecção exigidas no cenário de ameaças atual.

– Resposta Rápida: uma vez identificada uma ameaça, o tempo de resposta torna-se o fator crítico. Tal como nas batalhas navais, em que as ordens devem ser executadas prontamente para manobrar os navios para uma posição vencedora, na guerra cibernética as equipes de segurança devem isolar rapidamente os sistemas afetados, aplicar as correções necessárias em função da resiliência e executar protocolos de resposta para mitigar o impacto de um ataque.

– Preparação e Treinamento: assim como as tripulações navais treinam e se preparam para as batalhas, as equipes de segurança cibernética devem realizar exercícios regulares de treinamento e simulação. Estes preparativos contribuem para que a resposta da equipe seja a mais rápida e eficaz possível, minimizando hesitações e maximizando a continuidade operacional.

– Liderança Decisiva: em momentos de crise, uma liderança decisiva é fundamental. Tal como um comandante naval deve tomar decisões rápidas com informações incompletas, os líderes da guerra cibernética também devem tomar decisões rápidas com base nos dados disponíveis para superar os adversários deste domínio.

– Aplicação de Inteligência: Na guerra naval, a Inteligência sobre as localizações e planos do inimigo pode fornecer uma vantagem significativa. Da mesma forma, na guerra cibernética, a *threat intelligence* [4], ou inteligência de ameaças (tradução livre), desempenha um papel crucial na antecipação e preparação para potenciais ataques cibernéticos, permitindo aos defensores reforçarem as defesas ou neutralizarem, preventivamente, os ataques em curso.

Ao aplicar o princípio de Nelson, vemos que na guerra cibernética, tal como nas batalhas navais, a gestão eficaz do tempo, desde a detecção até a resposta, pode ser o fator decisivo entre proteger uma rede ou enfrentar um incidente cibernético com impactos catastróficos. Este ponto de vista destaca a necessidade de melhoria contínua nas estratégias de guerra cibernética, com foco na velocidade e na eficiência para garantir a resiliência e a vitória na era digital.

## *CLOCK DECISIONS*

O termo *clock decisions*, ou "decisões de relógio" (tradução livre), não se refere a um conceito específico e bem definido na gestão geral ou na literatura sobre a tomada de decisões estratégicas. No entanto pode ser interpretado com o significado de decisões que estão fortemente limitadas por restrições de tempo, em que o momento da decisão é crucial para o seu sucesso ou fracasso. Esta ideia pode ser aplicada em vários campos, incluindo negócios, operações militares, gestão de emergências e, particularmente, em ambientes de ritmo acelerado, como o comércio financeiro ou setores tecnológicos.

No contexto dos negócios e da gestão, *clock decisions* podem se referir a decisões que precisam ser tomadas dentro de um prazo específico ou àquelas em que o tempo afeta significativamente o resultado. Por exemplo, decidir o momento exato de lançar um novo produto para maximizar o impacto no mercado ou cronometrar uma fusão de empresa em função das condições financeiras ou de mercado podem ser vistos como *clock decisions*.

Nas operações militares, o termo alinha-se estreitamente com a necessidade de resposta rápida e com a importância estratégica do *timing* nas ações e reações. As decisões devem ser tomadas rapidamente em resposta a ameaças ou situações táticas, nas quais os atrasos podem levar ao fracasso ou a resultados significativamente piores.

## O TEMPO NAS OPERAÇÕES CIBERNÉTICAS

Nas operações cibernéticas, *clock decisions* referem-se ao processo de tomada de decisão rápido e crítico, necessário para gerenciar e responder com eficácia às ações contra as ameaças cibernéticas, sendo um conceito essencial para a compreensão do ambiente dinâmico e de alto risco em que operam os guerreiros cibernéticos, em que cada segundo pode influenciar o resultado das Operações Cibernéticas Defensivas e Ofensivas (OpCiberDef).

**A capacidade de responder a um ataque cibernético em tempo hábil, a partir de tomada de decisões célere, contribui para contenção imediata de um incidente**

A importância do *timing* nas Operações Cibernéticas Defensivas [5] não pode ser menosprezada. A capacidade de responder a um ataque cibernético em tempo hábil, a partir de um processo de tomada de decisões célere, contribui na contenção imediata de um incidente, evitando o efeito cascata do impacto para partes não afetadas da rede ou dos sistemas, o que é crucial para manter a continuidade operacional e proteger ativos informacionais críticos.

Tal como na defesa, o *timing* é crucial na execução de Operações Cibernéticas Ofensivas (OpCiberOfs) [5]. As decisões sobre quando empreender uma ação ofensiva cibernética, que alvos escolher e como coordenar as ações para atingir os objetivos estratégicos são tomadas cuidadosamente, considerando o momento adequado. Estas operações podem ser planejadas para maximizar os impactos durante um período operacional crítico de um adversário ou para se alinharem com outros movimentos estratégicos em contextos militares ou geopolíticos mais amplos. Consideram-se como características das *clock decisions* em operações cibernéticas:

– Sensível ao Tempo: estas decisões são marcadas pela necessidade de ação urgente. Atrasar uma decisão pode resultar em oportunidades perdidas ou riscos aumentados.

– Importância Estratégica: o impacto destas decisões estende-se muitas vezes para além dos resultados imediatos, afetando posições estratégicas ou o sucesso a longo prazo.

– Alta Pressão: devido ao prazo limitado, estas decisões são normalmente tomadas sob alta pressão, exigindo determinação e muitas vezes confiança em informações incompletas.

– Dependência de Dados: decisões eficazes muitas vezes dependem de dados em tempo real e da capacidade de analisar e agir rapidamente com base nessas informações.

## CONCLUSÃO

Na segurança cibernética, o *timing* é um ativo estratégico. A capacidade de responder rapidamente a incidentes, aplicar atualizações e adaptar-se a novas ameaças pode melhorar significativamente a postura de segurança de uma organização. O *timing* eficaz na segurança cibernética contribui para a proteção dos ativos de informação, demonstrando a necessidade de investimento em pessoas, processos e tecnologias que permitam a detecção e resposta rápidas para manter defesas cibernéticas robustas.

As *clock decisions* na guerra cibernética são implacáveis, exigindo escolhas rápidas e bem informadas que podem ter consequências de longo alcance. Este ambiente requer uma combinação de tecnologia avançada, pessoal qualificado e formação contínua para garantir a prontidão e a eficácia em face de ameaças cibernéticas constantes e em evolução. Tal como o sucesso do Almirante Nelson dependia da execução atempada das táticas navais, o sucesso na guerra cibernética depende do domínio da arte e da ciência da tomada de decisões rápidas e estratégicas.

🗁 CLASSIFICAÇÃO PARA ÍNDICE REMISSIVO:
<ARTES MILITARES>; Decisão; Tática;
<GUERRAS>; Guerra Cibernética;
<INFORMÁTICA>; Cibernética;

## REFERÊNCIAS

[1] MASEFIELD, J. *Sea life in Nelson's Time*, 2002.
[2] BRASIL. Exército. Estado-Maior. *Manual de Campanha – Guerra Cibernética*. EB70--MC-10.232. 1ª Edição. Brasília, 2017.
[3] GRIMES, R. *Manual de proteção contra* ransomware: Como criar um plano de segurança cibernética, 2022.
[4] WILHOIT, K.; OPACKI, J. *Operationalizing Threat Intelligence*: A guide to developing and operationalizing cyber threat intelligence programs, 2022.
[5] BRASIL. Doutrina Militar de Defesa Cibernética. Ministério da Defesa, Estado-Maior Conjunto das Forças Armadas. MD31-M-07. 2ª Edição. Brasília, 2023.