Simpósio Acadêmico de Segurança e Defesa Cibernética

20 de julho de 2022

Escola Superior de Guerra

Simpósio Acadêmico de Segurança e Defesa Cibernética

Rio de Janeiro

20 de julho de 2022

Apresentação

CDCiber

CGE

CCOC

Contra-Almirante ANDRÉ CONDE

Objetivo

Conhecer os conceitos de Inteligência Cibernética, a evolução das ameaças no Espaço Cibernético e algumas das ferramentas empregadas na Defesa Cibernética.

Agenda

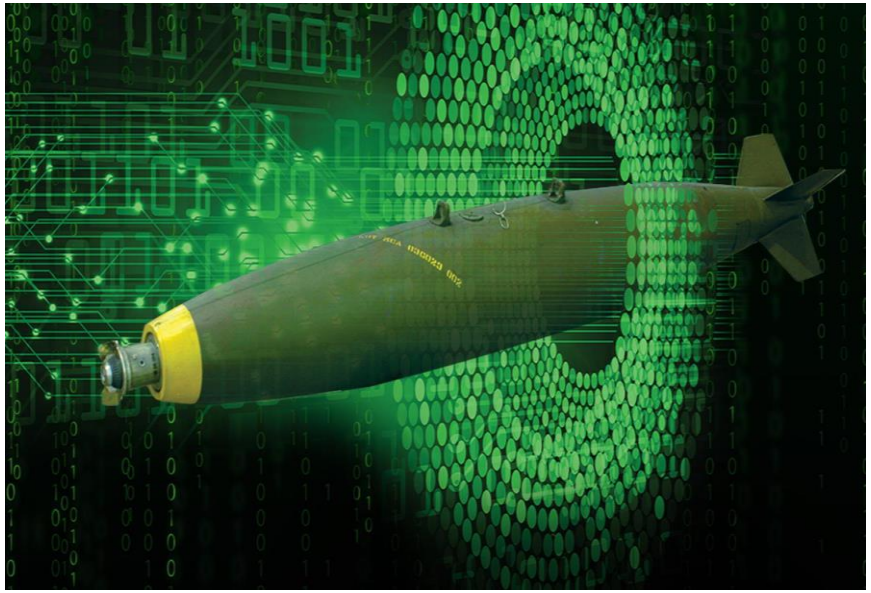
1. Introdução.
2. Conceitos de Inteligência Cibernética.
3. Ativos a proteger
4. Ameaças / Artefatos/Ataques
5. Exemplos de ferramentas de Defesa Cibernética
6. Considerações finais

Evolução da Estratégia Global

Guerra Fria

DISSUASÃO

Guerra Cibernética



RESILIÊNCIA

Resiliência Cibernética

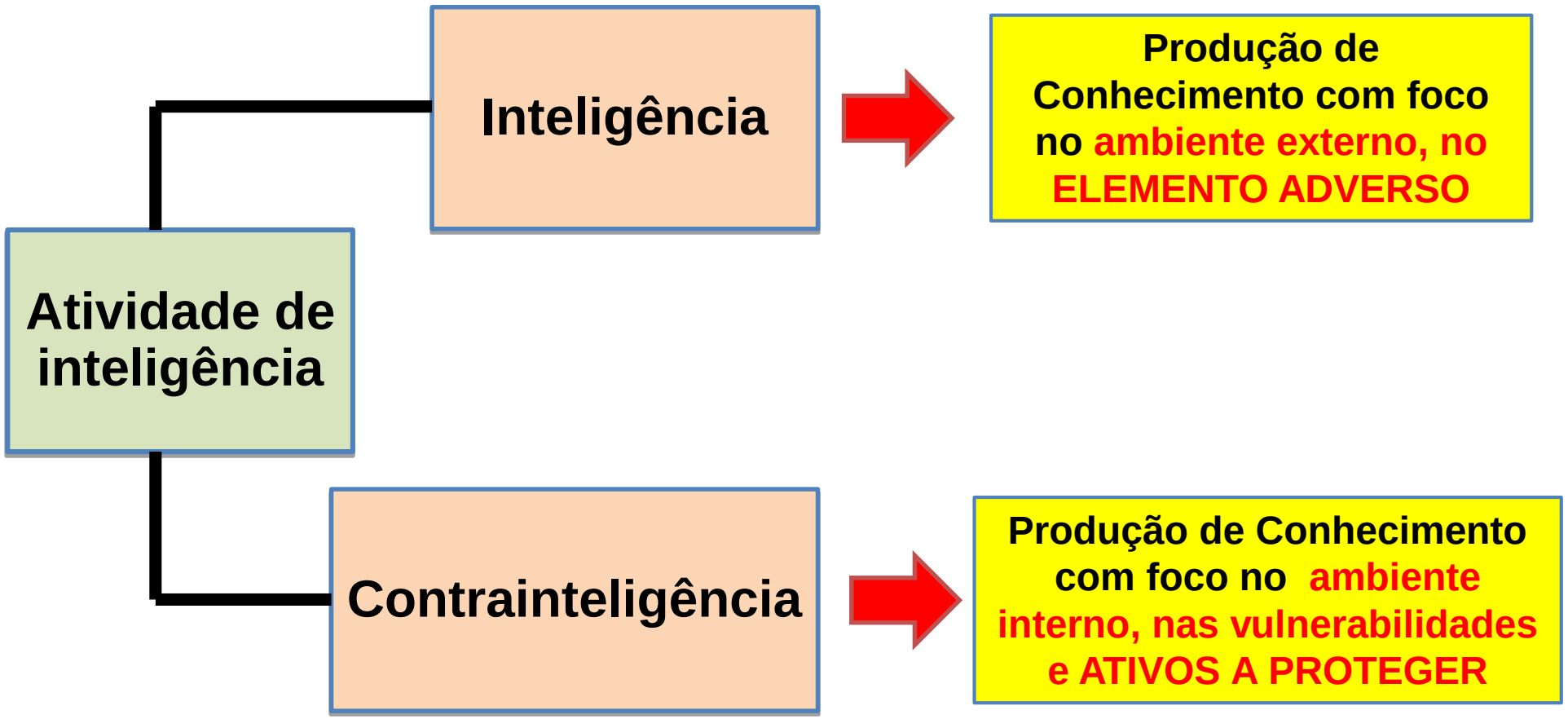
Capacidade de manter os ativos informacionais operando sob condições de ataque cibernético ou de restabelecê-los rapidamente após uma ação adversa.

(Doutrina Militar de Defesa Cibernética)

Agenda

1. Introdução.
2. Conceitos de Inteligência Cibernética.
3. Ativos a proteger
4. Ameaças / Artefatos/Ataques
5. Exemplos de ferramentas de Defesa Cibernética
6. Considerações finais

Ramos da Atividade de Inteligência



Fontes Cibernéticas x Inteligência Cibernética

Fontes Cibernéticas → **Qualquer ativo da informação pela qual se pode obter dados no espaço cibernético**

Conhecimento não necessariamente será usado no Espaço Cibernético

Inteligência Cibernética → **Produção de conhecimento a ser utilizado em prol de ações no Espaço Cibernético**

Fonte não necessariamente é cibernética (HUMINT, etc)

Inteligência Cibernética ↓

Inteligência de Ameaças Cibernéticas
(*Cyber Threat Intelligence* - CTI)

Níveis da Inteligência Cibernética

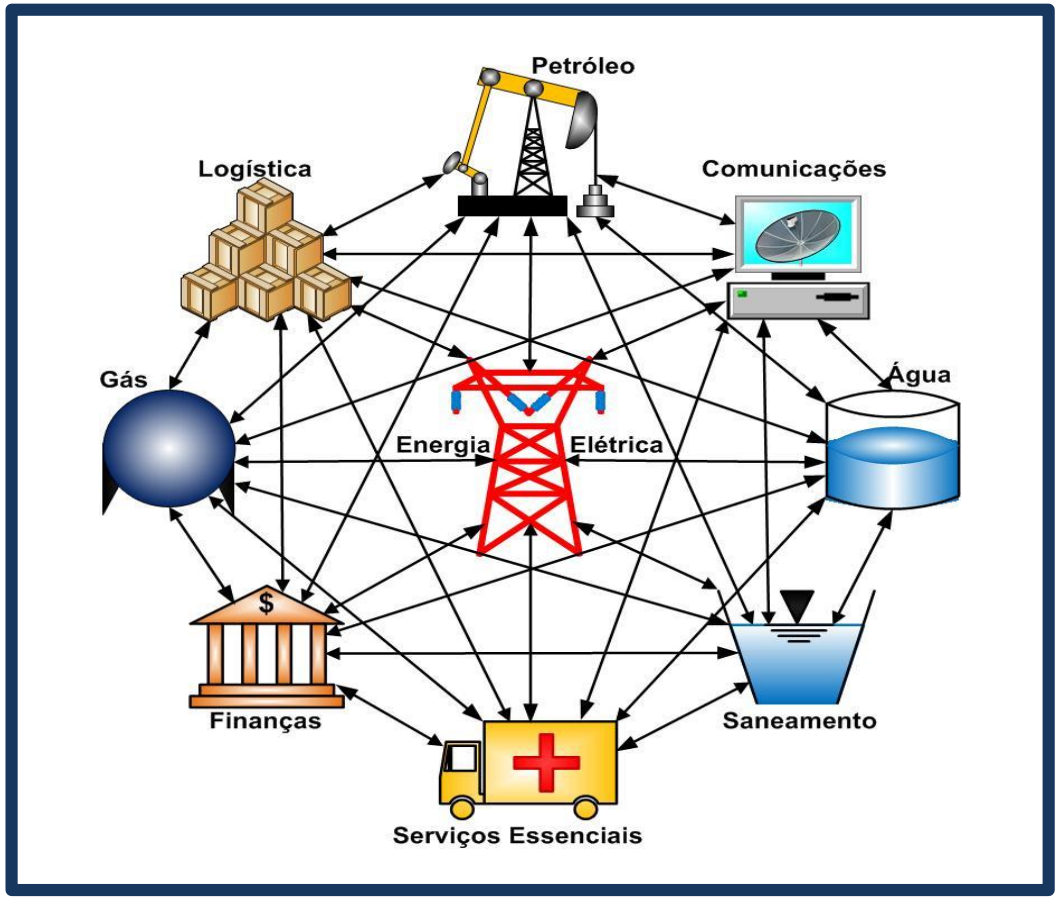
Inteligência Cibernética

- **Nível Estratégico** — Fatores motivadores das ameaças, tendências, contextos estratégicos
- **Nível Operacional** — *Modus Operandi* das Operações Cibernéticas do Adversário
- **Nível Tático** — Metodologia: Táticas, Técnicas e Procedimentos (TTP)

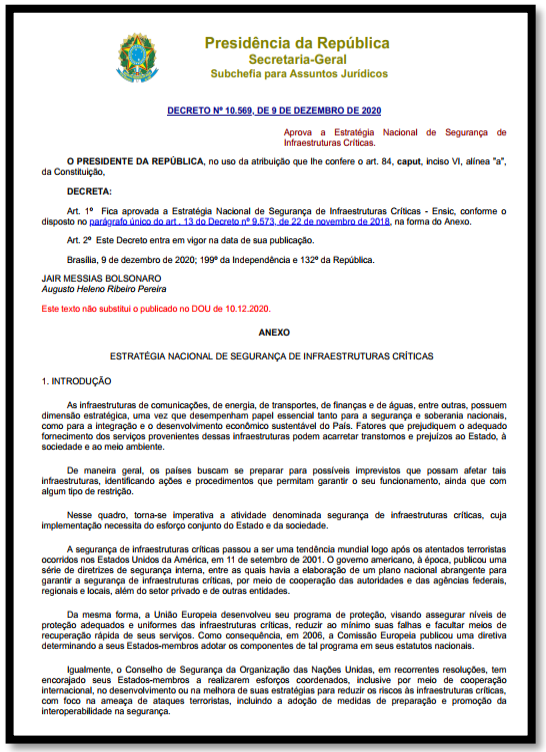
Agenda

1. Introdução.
2. Conceitos de Inteligência Cibernética.
3. Ativos a proteger
4. Ameaças / Artefatos/Ataques
5. Exemplos de ferramentas de Defesa Cibernética
6. Considerações finais

Infraestruturas Críticas



DEC 9.573/2018



Presidência da República
Secretaria-Geral
Subchefia para Assuntos Jurídicos

DECRETO Nº 10.569, DE 9 DE DEZEMBRO DE 2020

Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas.

O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 84, **caput**, inciso VI, alínea "a", da Constituição,

DECRETA:

Art. 1º Fica aprovada a Estratégia Nacional de Segurança de Infraestruturas Críticas - Ensic, conforme o disposto no parágrafo único do art. 13 do Decreto nº 9.573, de 22 de novembro de 2018, na forma do Anexo.

Art. 2º Este Decreto entra em vigor na data de sua publicação.

Brasília, 9 de dezembro de 2020; 199º da Independência e 132º da República.

JAIR MESSIAS BOLSONARO
Augusto Heleno Ribeiro Pereira

Este texto não substitui o publicado no DOU de 10.12.2020.

ANEXO

ESTRATÉGIA NACIONAL DE SEGURANÇA DE INFRAESTRUTURAS CRÍTICAS

1. INTRODUÇÃO

As infraestruturas de comunicações, de energia, de transportes, de finanças e de águas, entre outras, possuem dimensão estratégica, uma vez que desempenham papel essencial tanto para a segurança e soberania nacionais, como para a integração e o desenvolvimento econômico sustentável do País. Fatores que prejudiquem o adequado fornecimento dos serviços provenientes dessas infraestruturas podem acarretar transtornos e prejuízos ao Estado, à sociedade e ao meio ambiente.

De maneira geral, os países buscam se preparar para possíveis imprevistos que possam afetar tais infraestruturas, identificando ações e procedimentos que permitam garantir o seu funcionamento, ainda que com algum tipo de restrição.

Nesse quadro, torna-se imperativa a atividade denominada segurança de infraestruturas críticas, cuja implementação necessita do esforço conjunto do Estado e da sociedade.

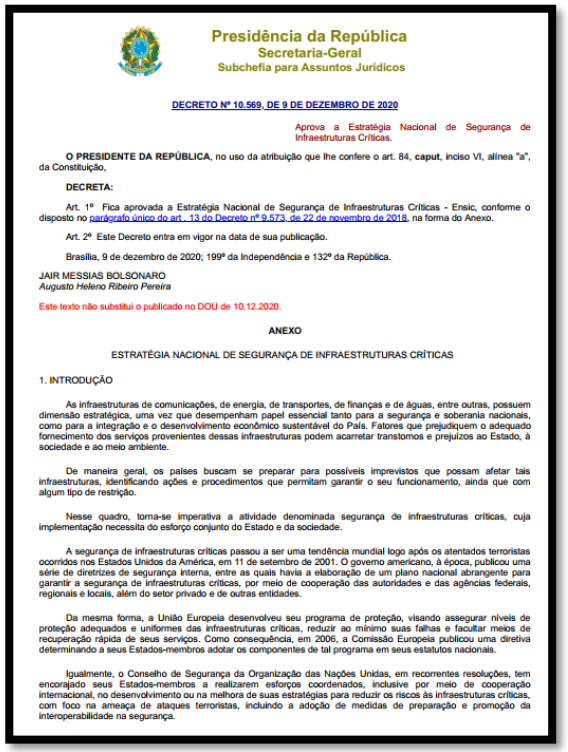
A segurança de infraestruturas críticas passou a ser uma tendência mundial logo após os atentados terroristas ocorridos nos Estados Unidos da América, em 11 de setembro de 2001. O governo americano, à época, publicou uma série de diretrizes de segurança interna, entre as quais havia a elaboração de um plano nacional abrangente para garantir a segurança de infraestruturas críticas, por meio de cooperação das autoridades e das agências federais, regionais e locais, além do setor privado e de outras entidades.

Da mesma forma, a União Europeia desenvolveu seu programa de proteção, visando assegurar níveis de proteção adequados e uniformes das infraestruturas críticas, reduzir ao mínimo suas falhas e facultar meios de recuperação rápida de seus serviços. Como consequência, em 2006, a Comissão Europeia publicou uma diretiva determinando a seus Estados-membros adotar os componentes de tal programa em seus estatutos nacionais.

Igualmente, o Conselho de Segurança da Organização das Nações Unidas, em recorrentes resoluções, tem encorajado seus Estados-membros a realizarem esforços coordenados, inclusive por meio de cooperação internacional, no desenvolvimento ou na melhora de suas estratégias para reduzir os riscos às infraestruturas críticas, com foco na ameaça de ataques terroristas, incluindo a adoção de medidas de preparação e promoção da interoperabilidade na segurança.

PNIC

DEC 10.589/2020



Presidência da República
Secretaria-Geral
Subchefia para Assuntos Jurídicos

DECRETO Nº 10.569, DE 9 DE DEZEMBRO DE 2020

Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas.

O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 84, **caput**, inciso VI, alínea "a", da Constituição,

DECRETA:

Art. 1º Fica aprovada a Estratégia Nacional de Segurança de Infraestruturas Críticas - Ensic, conforme o disposto no parágrafo único do art. 13 do Decreto nº 9.573, de 22 de novembro de 2018, na forma do Anexo.

Art. 2º Este Decreto entra em vigor na data de sua publicação.

Brasília, 9 de dezembro de 2020; 199º da Independência e 132º da República.

JAIR MESSIAS BOLSONARO
Augusto Heleno Ribeiro Pereira

Este texto não substitui o publicado no DOU de 10.12.2020.

ANEXO

ESTRATÉGIA NACIONAL DE SEGURANÇA DE INFRAESTRUTURAS CRÍTICAS

1. INTRODUÇÃO

As infraestruturas de comunicações, de energia, de transportes, de finanças e de águas, entre outras, possuem dimensão estratégica, uma vez que desempenham papel essencial tanto para a segurança e soberania nacionais, como para a integração e o desenvolvimento econômico sustentável do País. Fatores que prejudiquem o adequado fornecimento dos serviços provenientes dessas infraestruturas podem acarretar transtornos e prejuízos ao Estado, à sociedade e ao meio ambiente.

De maneira geral, os países buscam se preparar para possíveis imprevistos que possam afetar tais infraestruturas, identificando ações e procedimentos que permitam garantir o seu funcionamento, ainda que com algum tipo de restrição.

Nesse quadro, torna-se imperativa a atividade denominada segurança de infraestruturas críticas, cuja implementação necessita do esforço conjunto do Estado e da sociedade.

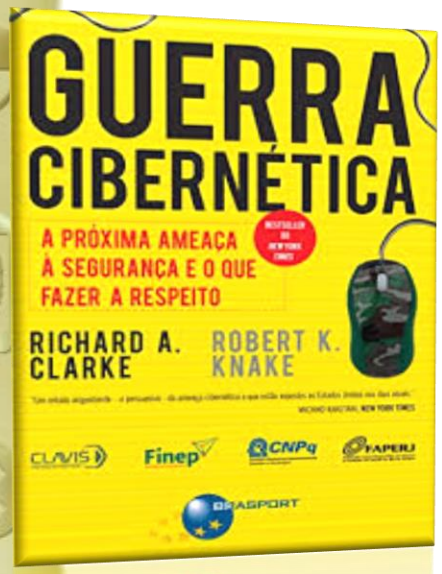
A segurança de infraestruturas críticas passou a ser uma tendência mundial logo após os atentados terroristas ocorridos nos Estados Unidos da América, em 11 de setembro de 2001. O governo americano, à época, publicou uma série de diretrizes de segurança interna, entre as quais havia a elaboração de um plano nacional abrangente para garantir a segurança de infraestruturas críticas, por meio de cooperação das autoridades e das agências federais, regionais e locais, além do setor privado e de outras entidades.

Da mesma forma, a União Europeia desenvolveu seu programa de proteção, visando assegurar níveis de proteção adequados e uniformes das infraestruturas críticas, reduzir ao mínimo suas falhas e facultar meios de recuperação rápida de seus serviços. Como consequência, em 2006, a Comissão Europeia publicou uma diretiva determinando a seus Estados-membros adotar os componentes de tal programa em seus estatutos nacionais.

Igualmente, o Conselho de Segurança da Organização das Nações Unidas, em recorrentes resoluções, tem encorajado seus Estados-membros a realizarem esforços coordenados, inclusive por meio de cooperação internacional, no desenvolvimento ou na melhora de suas estratégias para reduzir os riscos às infraestruturas críticas, com foco na ameaça de ataques terroristas, incluindo a adoção de medidas de preparação e promoção da interoperabilidade na segurança.

ENIC

O Brasil pode ser Alvo?



"De fato, em 2007, o especialista da CIA Tom Donahue foi autorizado a dizer em uma audiência pública para especialistas que a Agência estava ciente de ocorrências dessa natureza feita por *hackers*. Embora Tom não tenha mencionado onde os *hackers* causaram o apagão com um esquema criminoso, mais tarde foi revelado que o incidente ocorrera no Brasil.

O apagão de 2003 durou para a maioria das pessoas algumas longas horas, mas mesmo sem ninguém ter tentado prolongar o efeito, em alguns lugares ele

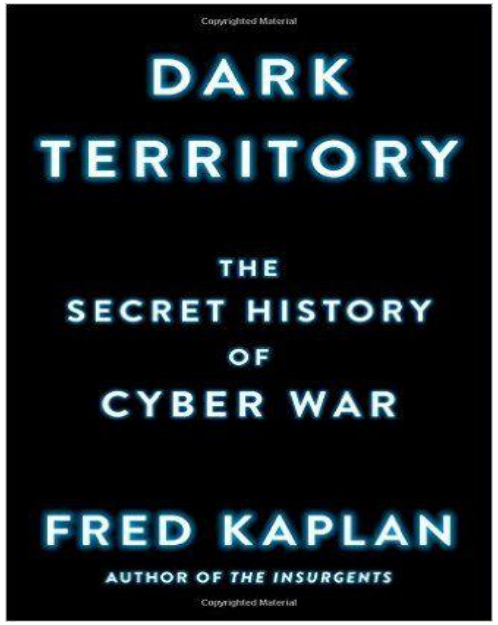
Agenda

1. Introdução.
2. Conceitos de Inteligência Cibernética.
3. Ativos a proteger
4. Ameaças / Artefatos/Ataques
5. Exemplos de ferramentas de Defesa Cibernética
6. Considerações finais

Evolução das Ameaças Cibernéticas

Evolução das Ameaças Cibernéticas

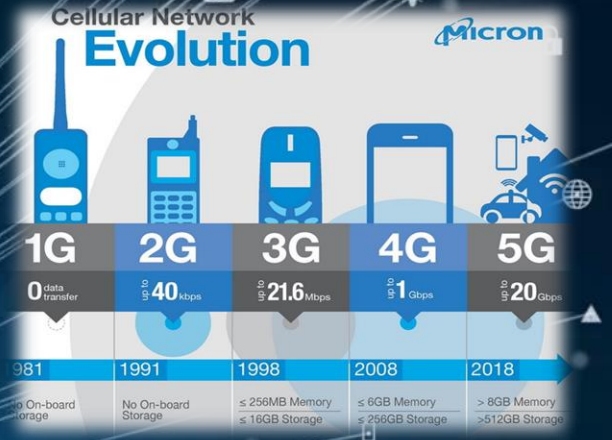
Século XX

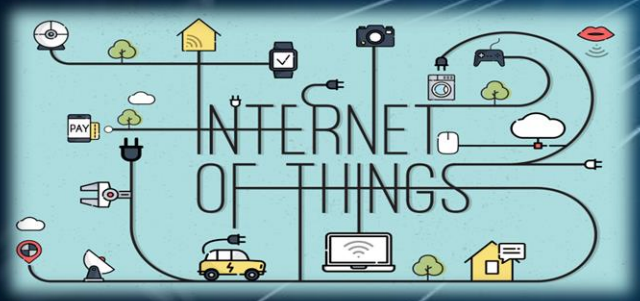


‘Em junho de 1983, o presidente Reagan assistiu ao filme Jogos de Guerra, no qual um adolescente involuntariamente “hackeia” o Pentágono, e pergunta ao seus generais se o cenário era plausível. O general disse que sim. Isso deu início à primeira diretriz presidencial sobre segurança de computadores. “*National Policy on Telecommunications and Automated Information Systems Security*.” ’

Evolução das Ameaças Cibernéticas

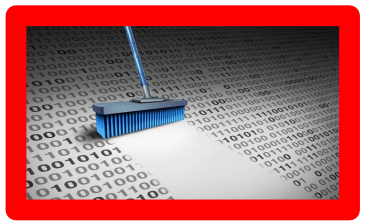
Século XXI





NOVAS TECNOLOGIAS...
NOVAS POSSIBILIDADES...
NOVAS AMEAÇAS...

ARTEFATOS CIBERNÉTICOS

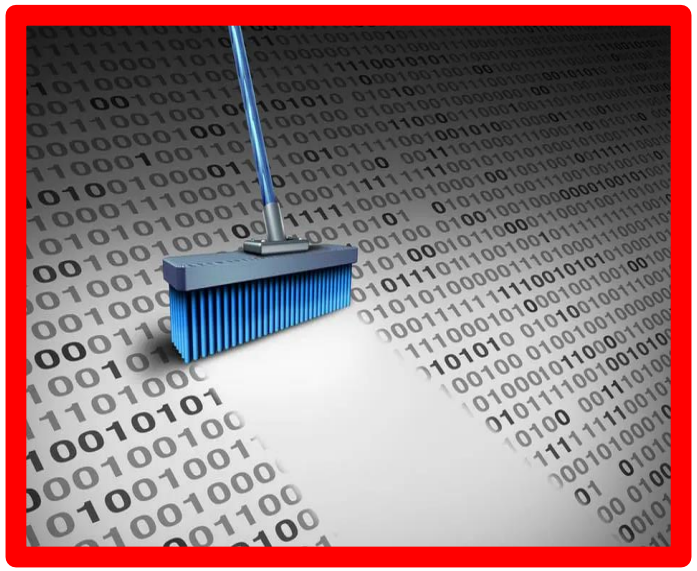


ARTEFATOS CIBERNÉTICOS

SPYWARE

O Spyware possui a função de espionar as atividades do usuário em seu dispositivo eletrônico. Ele coleta dados como pressionamentos de teclas (*keylogger*), hábitos de navegação e até informações de *login* que depois são enviados a terceiros, geralmente os criminosos virtuais.

ARTEFATOS CIBERNÉTICOS



WIPER

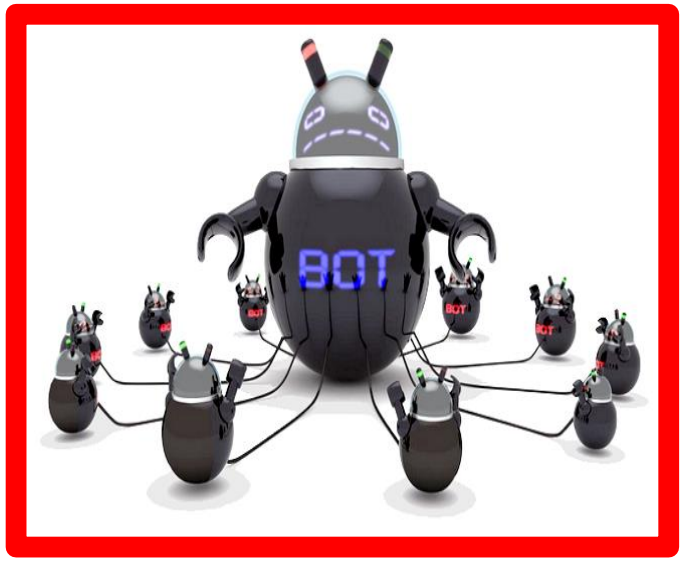
Um “Wiper” é uma classe de malware destinada a apagar (limpar) o disco rígido do computador que infecta, excluindo dados e programas maliciosamente.

ARTEFATOS CIBERNÉTICOS

RANSOMWARE

Ransomware é um *malware* que criptografa arquivos importantes no armazenamento local e de rede e exige um resgate para descriptografar os arquivos. Os atacantes desenvolvem esse *malware* para ganhar dinheiro com extorsão digital.

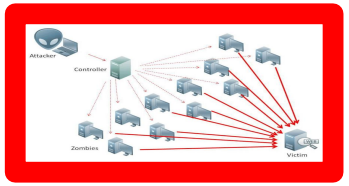
ARTEFATOS CIBERNÉTICOS



BOT

Bots, ou robôs da Internet, são também conhecidos como spiders, crawlers e bots da Web. Apesar de poderem ser usados para executar tarefas repetitivas, como a indexação de um mecanismo de pesquisa, eles normalmente adotam o formato de malware. Os bots de malware são usados para obter o controle total de um computador.

ATAQUES CIBERNÉTICOS

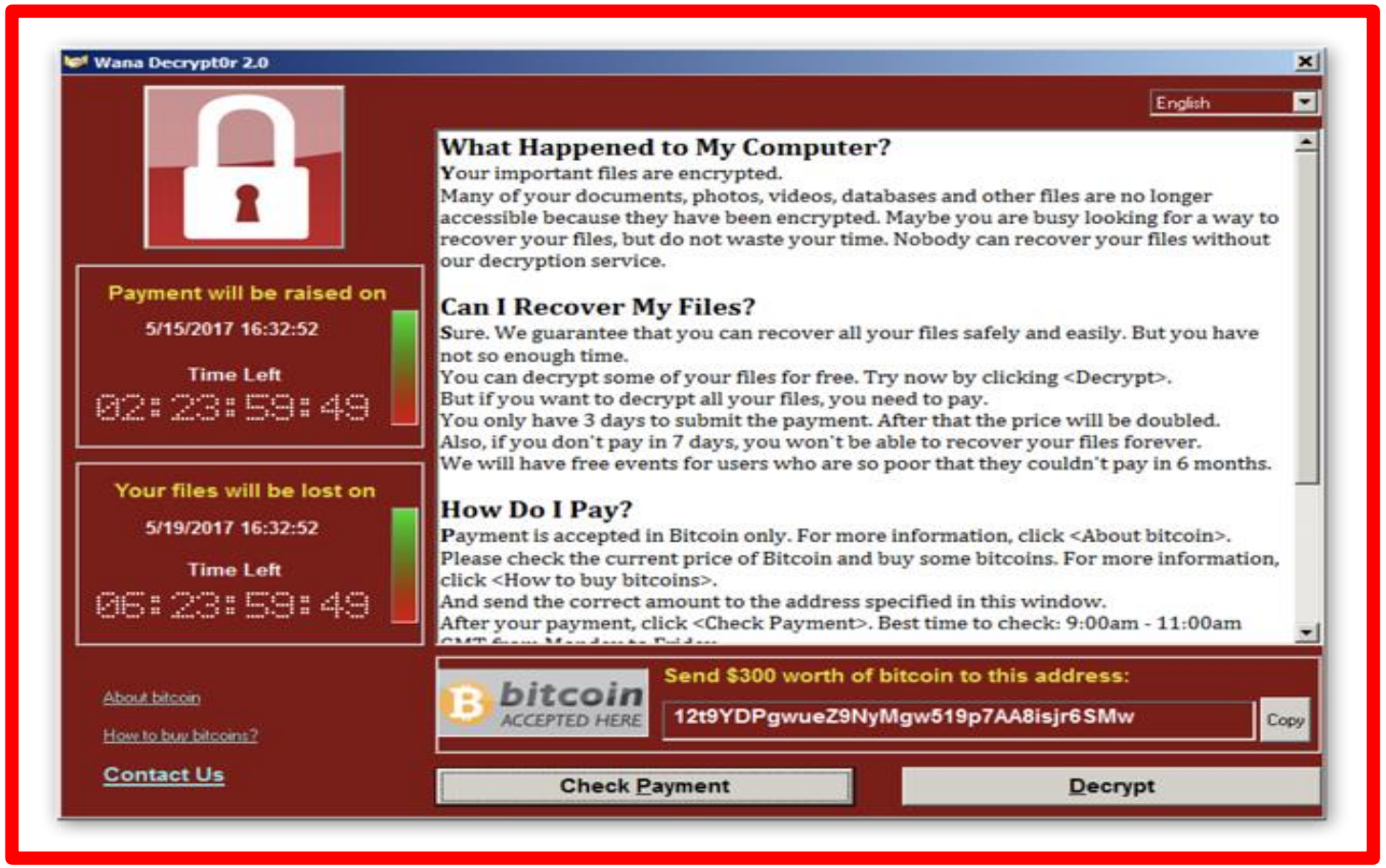


ATAQUES CIBERNÉTICOS

Phishing

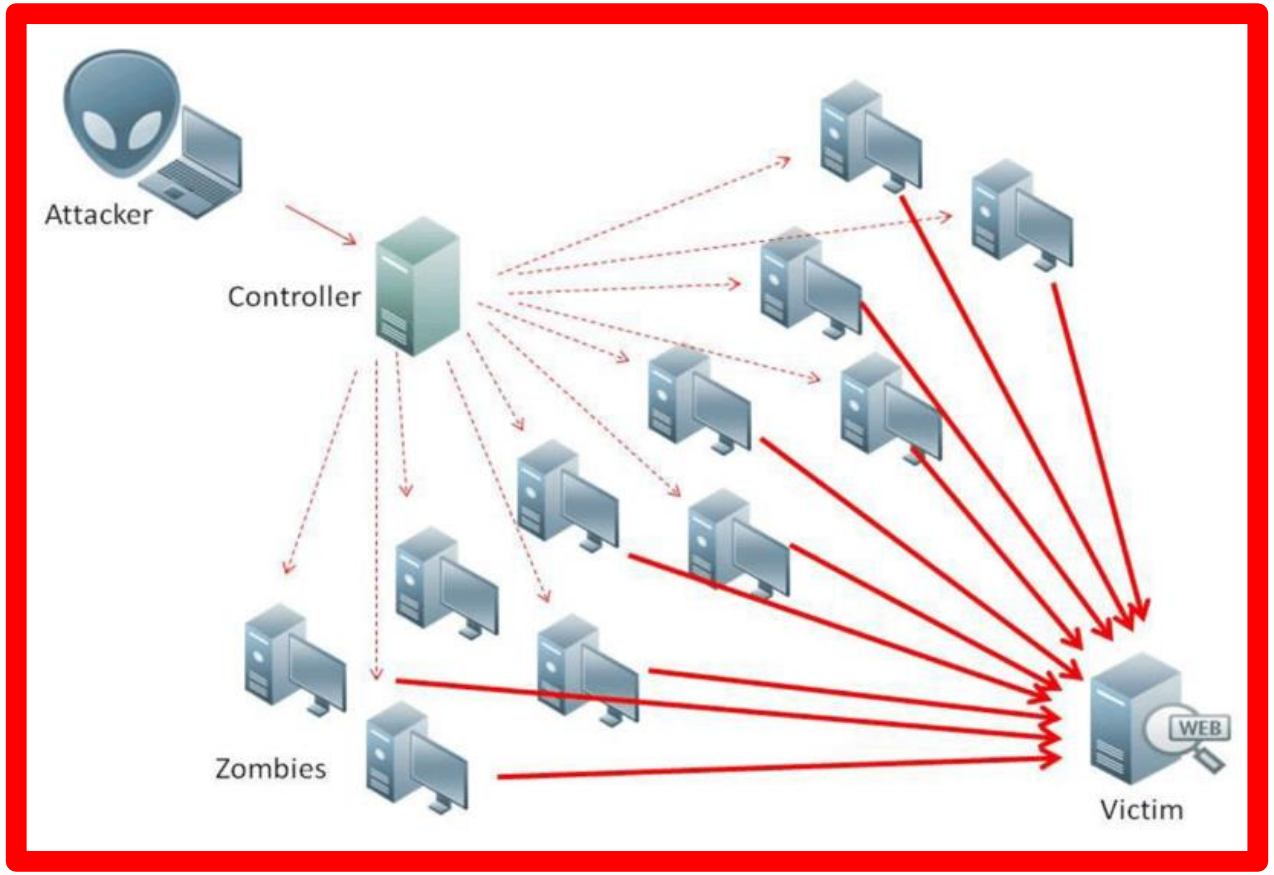
ATAQUES CIBERNÉTICOS

Sequestro de Dados



ATAQUES CIBERNÉTICOS

DDOS



Ataque de negação de serviço distribuído (*Distributed Denial-of-service attack)*

Advanced Persistent Threat (APT)

APT é a abreviatura de "*Advanced Persistent Threat*" (ameaça persistente avançada). Termo que se tornou famoso depois que o New York Times publicou, em 2013, detalhes do ataque que sofreu por mais de um mês. A unidade militar chinesa, agora conhecida como "APT 1", invadiu a rede da organização midiática com uma série de *e-mails* de *spear-phishing* e um dilúvio de *malwares* personalizados.

https://www.kaspersky.com.br/blog/o-que-e-apt/754/

https://www.hscbrasil.com.br/apt/

Advanced Persistent Threat (APT)

Uma ameaça persistente avançada difere dos tradicionais ataques cibernéticos por seu alto nível de complexidade, utilizando técnicas não muito conhecidas aliado a malwares desenvolvidos especialmente para um único ataque. Ela também é mais lenta e busca precisão ao atingir uma única brecha. Uma vez dentro da rede corporativa, permanece até obter o máximo possível de informações.

https://www.kaspersky.com.br/blog/o-que-e-apt/754/ https://www.hscbrasil.com.br/apt/

Advanced Persistent Threat (APT)

ANONYMOUS

APT 28 *FANCY BEAR*

APT 29 *COZY BEAR*

GRUPO CONTI

SANDWORM

GRUPO LAZARUS

Advanced Persistent Threat (APT)

CICADA

FUNNY DREAM

POSEIDON

DEEP PANDA

CHARMING KITTEN

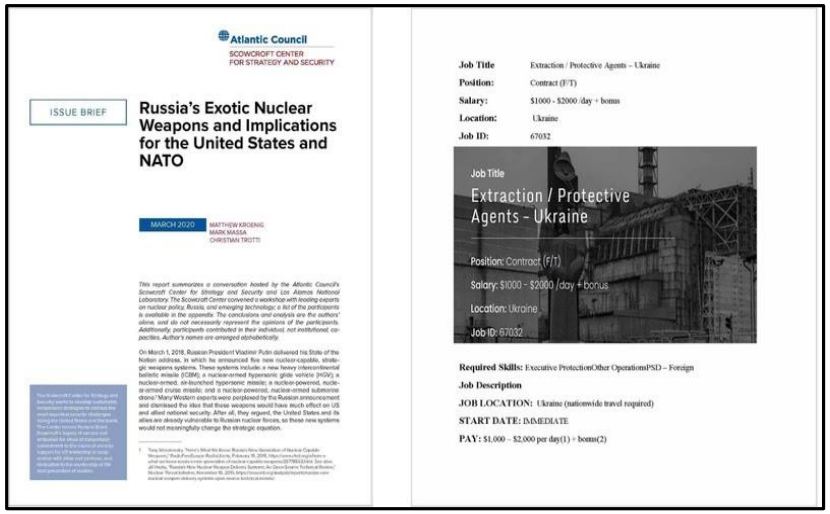
PRILEX

Espionagem Cibernética

“Hackers usam documentos sobre a guerra para ciberespionagem” 05/ABR/2022

Operadores de ameaças em todo o mundo estão utilizando documentos com temas sobre a Rússia e a Ucrânia para disseminar malware e atrair vítimas para espionagem cibernética

Nome do APT	Origem APT	Setor ao qual se destina	Países-Alvo
El Machete	Países que falam espanhol	Financeiro, Governo	Nicarágua, Venezuela
Lyceum	República Islâmica do Irã	Energia	Israel, Arábia Saudita
SideWinder	Possivelmente Índia	Desconhecido	Paquistão



Documentos atrativos relacionados com a guerra entre Rússia e Ucrânia utilizados pelo grupo Lyceum APT

https://www.cisoadvisor.com.br/hackers-usam-documentos-sobre-a-guerra-para-ciberespionagem/

Espionagem Cibernética

“O novo exército chinês invadiu e nós não estamos reagindo”

‘O exército secreto da China é considerável. O FBI acredita ter cerca de 30.000 ciberespiões militares e 150.000 hackers informais que ele pode convocar, e está alimentando um nova geração de “hackers patrióticos” para visar tecnologias futuristas nas quais a China quer liderar o mundo.’

The Sunday Times, 17 JUL 2022

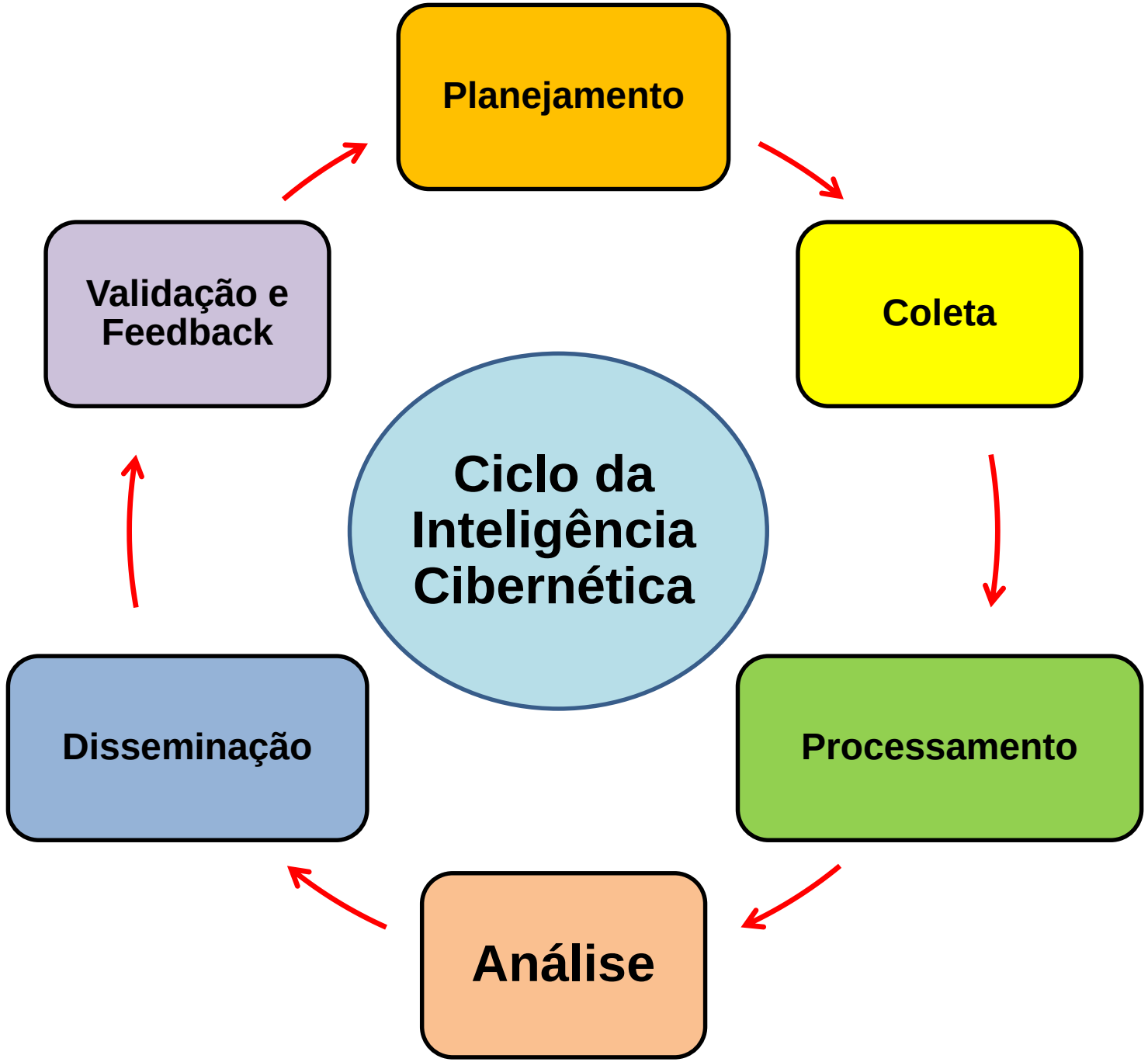
China’s new spy army has invaded — and we’re not fighting back

MI5 and the FBI have issued a warning that would be devastating to ignore, writes *Ian Williams*

China can call on some 150,000 amateur hackers

Agenda

1. Introdução.
2. Conceitos de Inteligência Cibernética.
3. Ativos a proteger
4. Ameaças / Artefatos/Ataques
5. Exemplos de ferramentas de Defesa Cibernética
6. Considerações finais


Planejamento
Coleta
Processamento
Análise
Disseminação
Validação e Feedback
Ciclo da Inteligência Cibernética

Ferramentas

MISP

MISP Threat Sharing

DARKWEB

Fonte de Dados

FRAMEWORKS

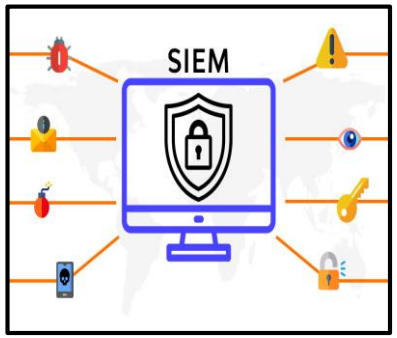
CYBER KILL CHAIN

ATT&CK

MITRE ATT&CK™

Modus Operandi

SIEM



Correlação de Eventos

NOC /SOC

Monitoramento

MALWARE INFORMATION SHARING PLATFORM - MISP

Ao todo, há **35 entidades públicas ou privadas** conectadas ao MISP do CDCiber:

- CERT.br
- CTIR.gov
- Órgãos de Defesa Cibernética de Nações Amigas (Peru, Uruguai, Chile e Portugal)
- Representantes dos Setores de Infraestruturas Críticas

TRAFFIC LIGHT PROTOCOL (TLP)

Cor	Restrição	Motivo
TLP:RED	Não deve ser divulgado, restrito somente aos participantes.	Informações que, se divulgadas, impactam a privacidade, reputação ou operação de uma organização.
TLP:AMBER	Divulgação limitada, restrita às organizações dos participantes.	Informações que, se divulgadas, impactam a privacidade, reputação ou operação de uma organização, mas que precisam do envolvimento de outras áreas.
TLP:GREEN	Divulgação limitada, restrito à comunidade.	Informação sem impacto, de interesse de uma organização ou setor
TLP:WHITE	Divulgação não é limitada	Informação de baixo risco se divulgada.

https://www.first.org/tlp/docs/tlp-v1-pt-br.pdf

INTERNET

SURFACE WEB

- Publicly available websites
- Search engines

DEEP WEB

- Medical information
- Legal documents
- Scientific reports
- Subscription info
- Various databases
- Government Intel
- Company specific repositories

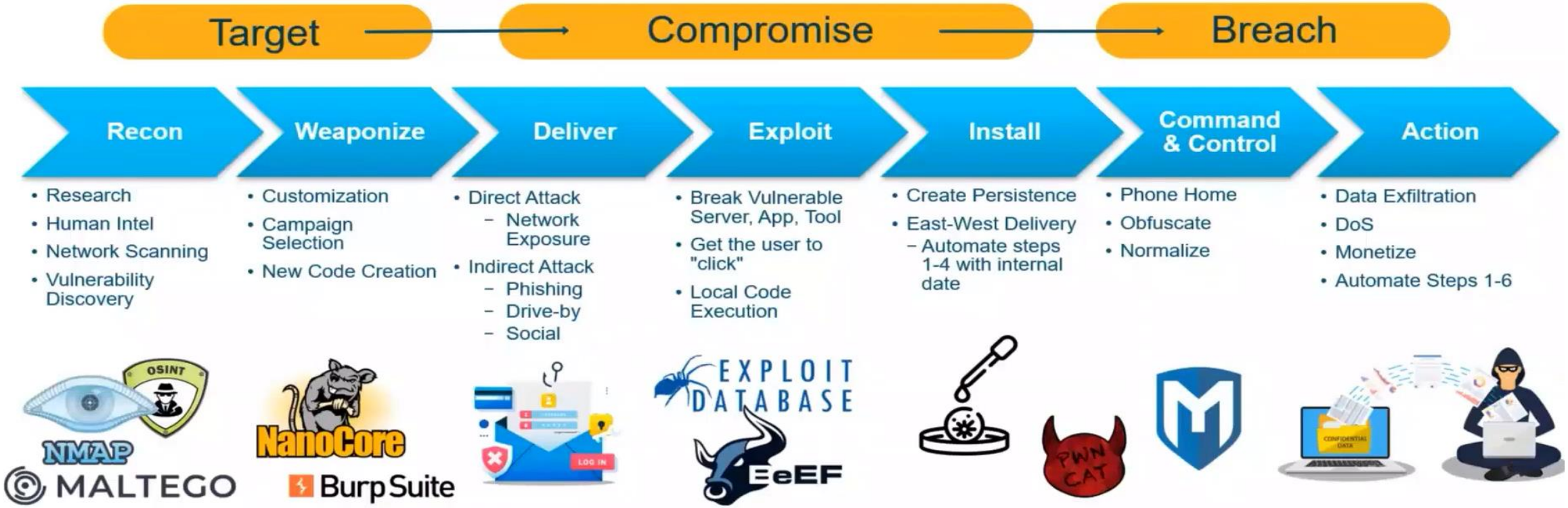
DARK WEB

- Illegal websites and information
- Tor-encrypted websites
- Websites that sell drugs
- Private communication forums

Quebrando a Cadeia

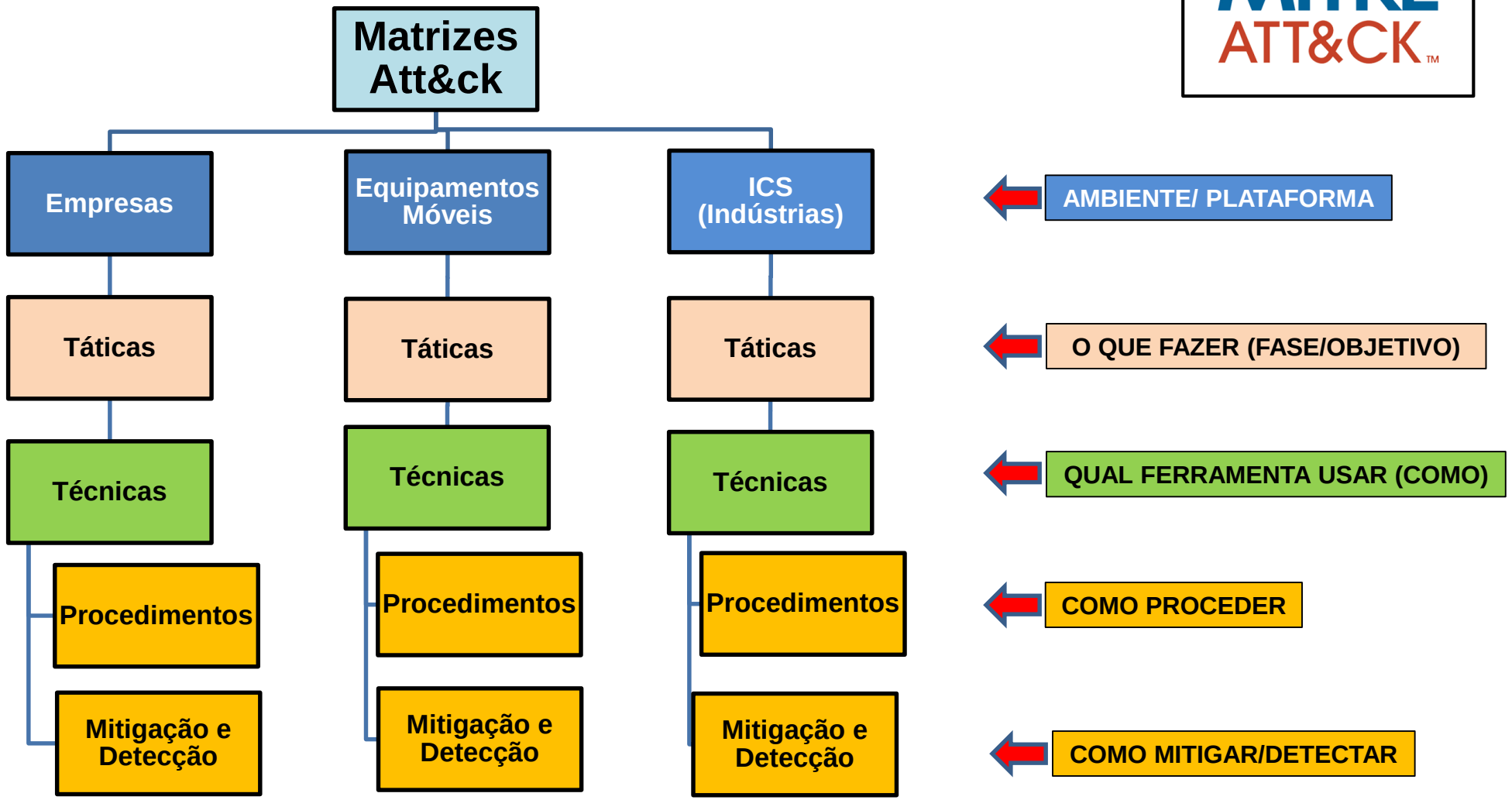
Lockheed Martin- *CYBER KILL CHAIN*

Lockheed Martin- *CYBER KILL CHAIN*



Entender a "Kill Chain" é o início do entendimento de quais tipos de eventos vão "expor" o ataque. (Indicadores de Ataque e Indicadores de Comprometimento)

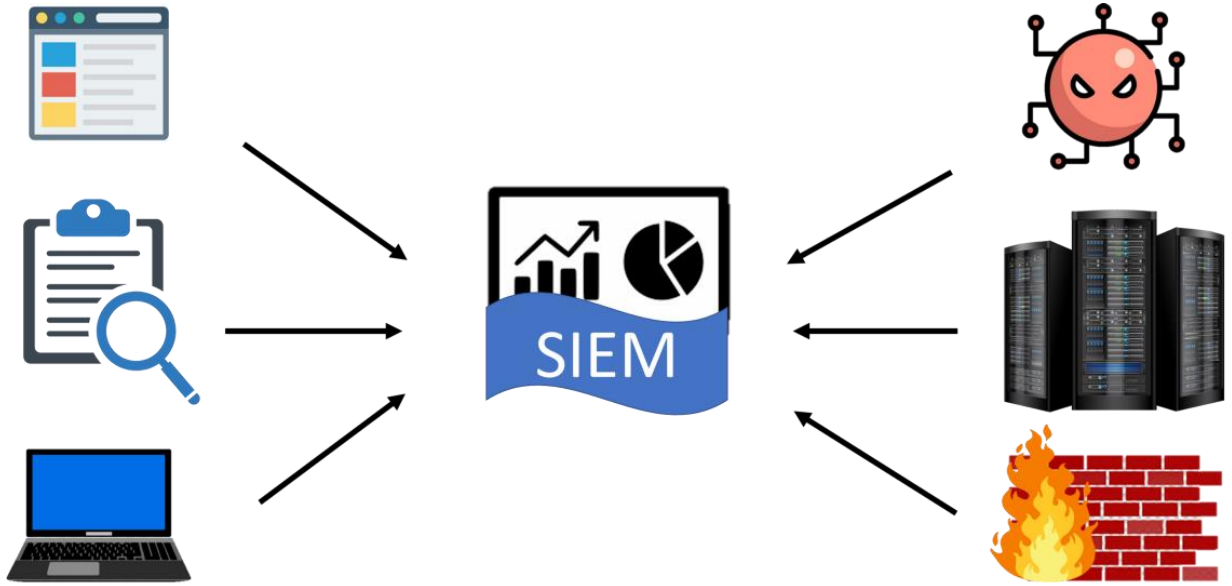
MITRE - ATT&CK



https://attack.mitre.org/

SIEM

Security Information and Event Management



Os alertas serão acionados se o mecanismo de análise da ferramenta detectar atividades que violam um conjunto de regras, sinalizando, consequentemente, um problema de segurança.

SOC/ NOC

SOC- *Security Operations Center* ou **Centro de Operações de Segurança**

Foco na Segurança da informação e dos dados

NOC - *Network Operations Center* ou **Centro de Operações de Rede**

Foco no Desempenho e disponibilidade da REDE


Ciclo da Inteligência Cibernética
Planejamento
Coleta
Processamento
Análise
Disseminação
Validação e Feedback
MITRE ATT&CK
MISP Threat Sharing
SIEM

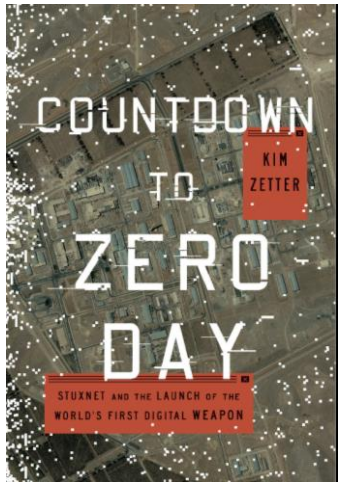
Agenda

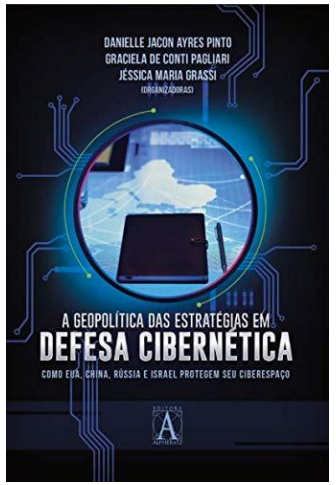
1. Introdução.
2. Conceitos de Inteligência Cibernética.
3. Ativos a proteger
4. Ameaças / Artefatos/Ataques
5. Exemplos de ferramentas de Defesa Cibernética
6. Considerações finais

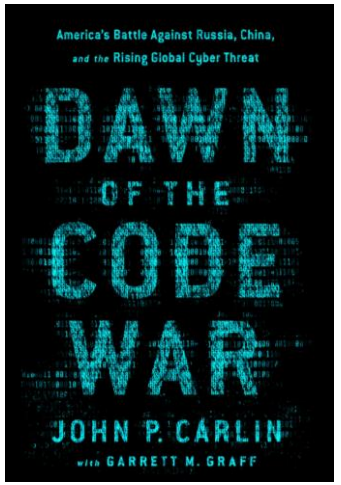
Considerações finais

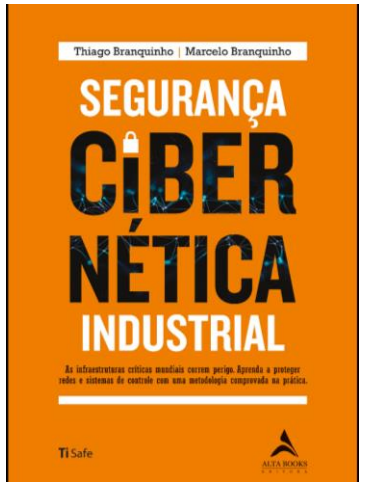
- Conceito de Inteligência Cibernética
  - Conhecimento empregado no Espaço Cibernético
- Evolução das Ameaças Cibernéticas
  - Amadorismo dos “piratas de computador”
  - Profissionalismo das APT
- Ferramentas de Inteligência Cibernética
  - Cooperação é fundamental
  - Defesa proativa

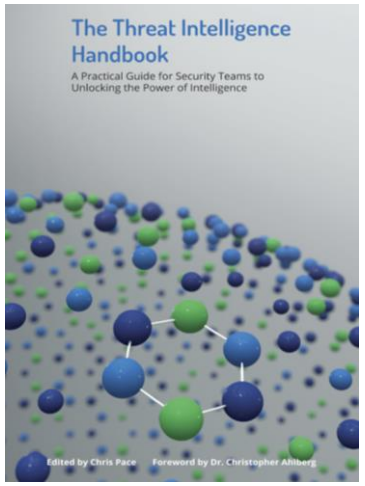
Considerações finais

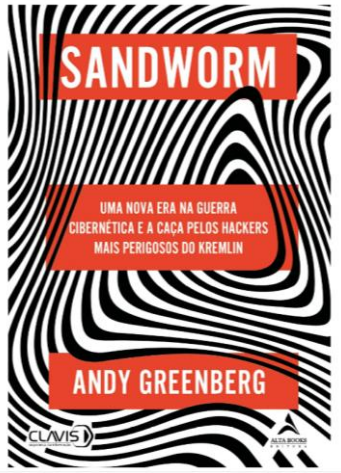












Considerações finais

*"Se você **conhece** o **inimigo** e conhece a **si mesmo**, não precisa temer o resultado de cem batalhas.*
*Se você **se conhece** mas **não conhece** o **inimigo**, para cada vitória ganha sofrerá também uma derrota.*
*Se você **não conhece** nem o **inimigo nem a si mesmo**, perderá todas as batalhas*."

Sun Tzu

“Uma nova visão do Espaço Cibernético”

PRIMEIRO, CIBERNÉTICA!

Deorse sagittarium ante deflectens sagitta

"Derrube o arqueiro em vez de desviar das flechas"

EFETIVIDADE – PRONTIDÃO – RESILIÊNCIA

andre.conde@marinha.mil.br

(61) 3415-3603