ESPIONAGEM E CONTRAESPIONAGEM

EM CAMPANHAS ELEITORIAIS

EDIÇÃO ESPECIAL

“Não será vantajoso para o exército agir sem conhecer a situação do inimigo, e conhecer a situação do inimigo não é possível sem espionagem**.”**

Sun Tzu

MIRAR

Que o militante conheça as técnicas de espionagem e - contraespionagem para que possa utilizá-las na sua campanha eleitoral e assim desenvolver uma estratégia baseada neste conhecimento.

ENDEREÇADO A:

Líderes políticos, gestores de marketing, publicitários, relações públicas, integrantes de campanhas eleitorais, pesquisadores e qualquer pessoa interessada em saber como a ferramenta empresarial WhatsApp pode ser utilizada para o relacionamento entre os integrantes de uma equipe e seu público.

ÍNDICE

CAPÍTULO I

FUNDAMENTOS TEÓRICOS

1.1 ESPIONAGEM

Definimos espionagem como aquilo que consiste em "*obter ou coletar informações quase secretas sobre política, recursos militares, organização de forças defensivas ou ofensivas*. Nesse sentido, a espionagem faz parte da inteligência estratégica, pois assim como Sherman Kent afirma o é". a busca por conhecimento útil.

A **Direcção Nacional de Inteligência (DINI**) define espionagem como o *"Conjunto de actividades de obtenção clandestina da nossa informação classificada, cujo conhecimento constitui um elemento valioso de julgamento para decisões que ameaçam a segurança da* **ACN***"*. ser de código aberto ou de código fechado.

Ciaran Martín, **chefe do Centro Nacional de Cibersegurança do Reino Unido,** afirma que *"o roubo de informações para fins políticos ou económicos é tão antigo quanto a humanidade".*

A espionagem é considerada uma estratégia de guerra, que está intimamente relacionada com a inteligência e as operações psicológicas. Portanto, para conhecer a relação entre inteligência e operações psicológicas, é importante e necessário conhecer o conceito de cada uma delas.

REGRA

1.2 A INTELIGÊNCIA

A inteligência a que nos referimos é aquela que todo estrategista deve possuir, e não a classificação dada pela psicologia, por isso os conceitos de inteligência na área militar são fundamentais, pois é aí que ela começa a ser utilizada em conjunto com a estratégia, na. desta forma a metodologia seria posteriormente adaptada a outras áreas.

Washington Platt, de uma perspectiva militar, definiu inteligência como *"um termo específico e significativo, derivado de informação, relatório, facto ou dados que foram seleccionados, avaliados, interpretados e finalmente expressos". (Pág.30)*

Por esse motivo, pode-se afirmar que a inteligência é o resultado de um processo de coleta de dados selecionados. Esta definição ainda é válida e é considerada por diversas escolas militares, no entanto, este conceito também foi adaptado a diversas áreas, uma vez que a inteligência estratégica segundo Platt não é aplicada apenas na guerra, mas também na paz.

Da mesma forma, **Karl Von Clausewitz** em seu livro Guerra aborda com maior profundidade sobre a guerra e as estratégias nela utilizadas, pois, embora o propósito da guerra seja a destruição do adversário, para atingir esse objetivo, a vários mecanismos, Clausewitz recorre à inteligência que desempenha um papel crucial na guerra, pois através dela são executadas as estratégias para atingir o objetivo traçado.

O conceito que lhe foi atribuído na **Direcção Nacional de**

Carlos Von Clausewitz

Inteligência do Peru (DINI) no âmbito da defesa nacional: "*É o conhecimento das ameaças à segurança nacional e seus correspondentes cenários de risco, fornecido para a tomada de decisões e a proteção de ativos críticos" (2014, p. 17)*.

Este conceito está ligado à noção dos autores acima mencionados, pois pelo exposto entende-se que a obtenção desse conhecimento será um produto do processo de análise da informação que será muito útil para os responsáveis pela tomada de decisões.

1.3 CONTRAESPIONAGEM

A **Direção Nacional de Inteligência (DINI)** define a contraespionagem: "O seu objetivo é prevenir ou neutralizar uma operação de inteligência humana ou técnica destinada a obter informação classificada sobre a **ACN**. Simultaneamente, a operação de contraespionagem cria a oportunidade de reunir informações sobre o agente da espionagem."

Para Sepúlveda, a contrainteligência consiste em:

> Combater as atividades dos espiões inimigos, localizando-os para anulá-los; Ele é responsável por monitorar os próprios agentes para que não se corrompam e verificar a veracidade de suas informações e a fidelidade de seus procedimentos; Ele deve evitar a sabotagem e a propaganda que o inimigo possa desenvolver, e é responsável pela tediosa mas importante tarefa da censura postal e telegráfica.

De acordo com o Manual de **Campo nº 2.0,** a contrainteligência consiste em neutralizar os esforços de coleta de inteligência, por meio de ações tomadas para detectar, identificar, explorar e neutralizar as atividades multidisciplinares de inteligência de amigos, concorrentes, oponentes, adversários e inimigos.

Ao descobrir os planos de espionagem que nossos adversários estão desenvolvendo, a criação de uma prática para neutralizar esses atos é chamada de contraespionagem ou contrainteligência, esta é desenvolvida através de diversas instituições com o objetivo de salvaguardar nossos dados mais importantes.

1.4 CICLO DE INTELIGÊNCIA

O ciclo de inteligência é o processo pelo qual as informações são -obtidas.
O **centro nacional de inteligência da Espanha (CNI**) entende o ciclo de inteligência como a sequência pela qual a informação é obtida, transformada em inteligência e disponibilizada aos usuários.

Segundo a **CNI,** seria composto por quatro fases:

- Endereço.
- Obtenção
- Elaboração.
- Difusão

Para a agência **central de inteligência (CIA),** é classificado em cinco fases:

- Planejamento e direção.
- Coleção.
- Acusação.
- Análise e produção.
- Difusão.

Diego Navarro Bonilla, em seu livro *O ciclo da inteligência e seus limites*, classifica a inteligência da seguinte forma:

- Planejamento e direção.
- Obtenção de informações.
- Processo.
- Análise e produção.
- Difusão e integração.
- Evolução e feedback.

Apresentamos vários ciclos de inteligência, de vários autores e instituições internacionais para mostrar que a metodologia utilizada para obter informação é semelhante em vários países, portanto a obtenção e processamento de informação será a mesma para nós e para os nossos adversários.

CAPÍTULO II

EVOLUÇÃO HISTÓRICA

Ciaran Martín, chefe do Centro Nacional de Cibersegurança do Reino Unido, afirma que “o roubo de informações para fins políticos ou económicos é tão antigo quanto a humanidade”.

Os princípios da espionagem remontam à Mesopotâmia, onde **Sargão I de Akkad** controlava um importante território no Mediterrâneo e no Golfo Pérsico. Ele criou uma rede de espiões que eram comerciantes que o informaram sobre as características dos territórios e civilizações que pretendia dominar.
O primeiro tratado militar que se refere à espionagem surgiu no império chinês com o livro **A Arte da Guerra** de **Sun Tzu** em que afirma que *“a melhor vitória é vencer sem lutar”*, afirmando também que existem cinco tipos de espiões que são :

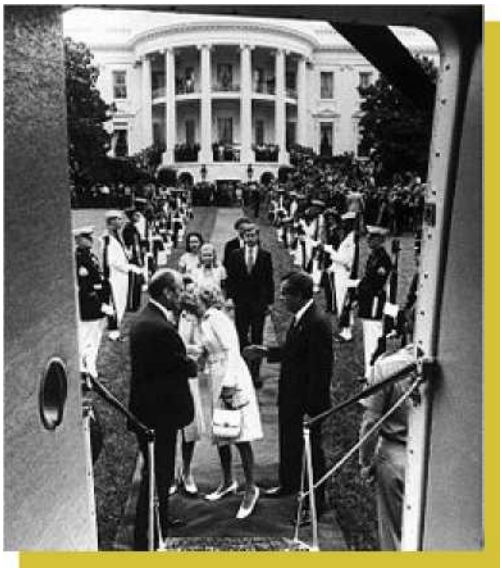
- **Espiões nativos:** são contratados entre os habitantes de uma localidade.
- **O espião interno:** era aquele que estava entre os oficiais do inimigo.
- **O agente duplo:** são contratados entre espiões inimigos.
- **O espião liquidável**: é aquele que transmite dados falsos a espiões inimigos.
- **Os espiões flutuantes:** são aqueles que só voltam para dar seus relatórios.

Também destaca a importância do conhecimento e da informação antes do combate.

Com o passar dos anos, a espionagem profissionalizou-se e -centralizou-se no Império Espanhol. **O Conselho de Estado**, -responsável pela nomeação dos embaixadores no estrangeiro, era supervisionado pelo Secretário de Estado e desempenhou um papel fundamental. Imediatamente abaixo disso, foi criado um cargo de renome: espião sênior da corte e superintendente de inteligência secreta.

Na **Primeira Guerra Mundial,** os países adversários utilizaram a espionagem; com os avanços tecnológicos, a interceptação de comunicações passou a ser utilizada. No final do século XIX, a Rússia

czarista criou uma das agências de inteligência mais eficazes. Inicialmente, surgiu como um serviço de segurança para a família real, aos poucos tornou-se uma verdadeira polícia secreta dedicada a desmascarar e oprimir os movimentos políticos revolucionários. .



Em 1974, **Richard Nixon utilizou a CIA** e os seus métodos de - espionagem para obter ganhos políticos pessoais. Essas atividades encobertas e ilegais acabaram explodindo em suas mãos e forçando-o a renunciar ao cargo de presidente dos Estados Unidos.

A espionagem na política profissionalizou-se e isso se deve aos escândalos de interceptação telefônica e de fotografias e/ou vídeos de candidatos realizando algumas ações que prejudicam sua imagem pública.

CAPÍTULO III

CARACTERÍSTICAS E TIPOS DE ESPIONAGEM

As técnicas mais comuns de espionagem são infiltração e penetração:

· **Infiltração:** é a técnica utilizada para introduzir sujeitos nas fileiras do adversário para que nos forneçam informações sobre suas atividades, capacidades, projetos, planos, etc. Pode-se dizer também que é a ação que consiste na utilização de uma pessoa, conhecida como toupeira, cujo objetivo é conquistar a confiança de quem tem a informação para ter acesso a ela.

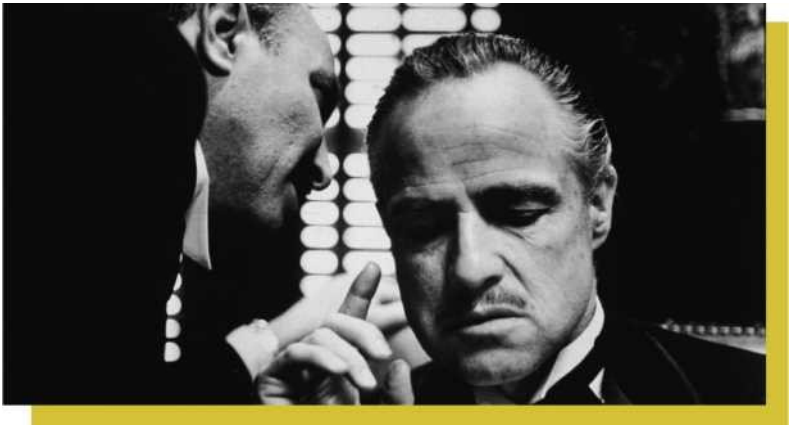
· **Penetração:** é uma técnica que consiste em conseguir a colaboração consciente ou inocente de um membro da organização ou grupo adversário para que forneça dados e informações confidenciais do grupo ao qual pertence. Esta acção é normalmente realizada de forma encoberta e emprega pessoas que foram persuadidas a trabalhar secretamente contra a sua própria organização por diversas motivações: ideológicas, económicas, religiosas, morais ou pessoais.

REGRA

Os espiões possuem várias técnicas para obter informações por dois meios:

- **O suborno** consiste na comparação de informações com dinheiro ou outros meios, como a força. Este método é amplamente utilizado na técnica de penetração.

- Caso se utilize **coerção** para obtê-lo, essa técnica é chamada de chantagem. Informações pessoais geralmente são usadas para forçar colaboradores.



3.1 TIPOS DE ESPIONAGEM

A classificação da espionagem gira em torno dos propósitos e meios utilizados, sendo os mais comuns a espionagem industrial e a espionagem cibernética.

· **A espionagem industrial** refere-se à obtenção ilícita de informações relacionadas com a investigação, desenvolvimento e fabrico de protótipos através dos quais as empresas pretendem sair à frente dos seus concorrentes na colocação de um produto inovador no mercado.

· **Espionagem cibernética:** esta prática se desenvolveu nos últimos anos do século devido à globalização e ao fácil acesso e uso massivo da Internet.

CAPÍTULO IV

CLASSIFICAÇÃO DE INTELIGÊNCIA

A classificação de inteligência que levaremos em consideração será a da **Doutrina de Inteligência** Nacional, visto que a espionagem utiliza estes quatro tipos de inteligência, temos que levar em conta que a atividade de espionagem é clandestina e requer uma grande quantidade de recursos humanos. , tecnológico e econômico.

REGRA

4.1 POR SEU NÍVEL DE APLICAÇÃO

- **Estratégico:** é produzido para o mais alto nível do Estado com o objetivo de tomar decisões nos níveis político e estratégico diante de ameaças.

- **Operacional:** produzido para fornecer o conhecimento preciso, compreensível e oportuno sobre ameaças e níveis de risco que um líder do setor necessita para planejar, preparar e executar suas operações ou atividades.

- Tática: produzida para fornecer conhecimento preciso, compreensível e tempestivo sobre riscos específicos em operações e ações a serem executadas pelos órgãos competentes.

REGRA

4.2 PELO SEU CONTEÚDO

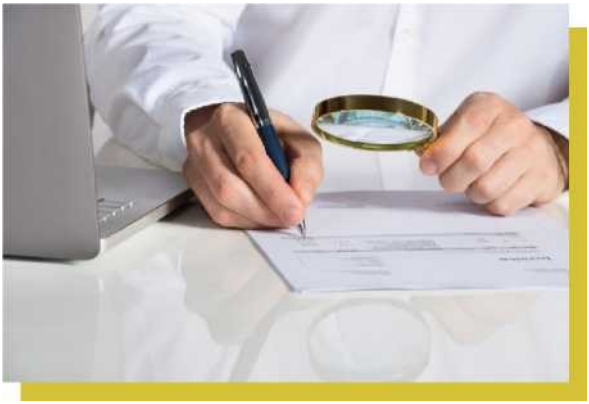
- Básico: é aquele que é atualizado e produzido de forma conveniente, contendo conhecimentos enciclopédicos úteis para o estudo de cenários de risco. Portanto, serve de insumo para o desenvolvimento da inteligência atual e preditiva.

- Atual: mostra e explica a situação e as mudanças que ocorrem no presente, bem como o seu futuro imediato e as atitudes dos autores envolvidos. É complementado com o conhecimento da inteligência básica.

- Preditivo: procura estabelecer as linhas de evolução dos cenários de risco e surgimento de novos cenários, com o objetivo de reduzir a incerteza no cumprimento dos objetivos. É influenciado pela inteligência básica e atual.

4.3 PELOS MEIOS EMPREGADOS

- Humano: obtido de fontes humanas. É útil porque fornece informações impossíveis de adquirir em outras mídias. Também fornece as ferramentas necessárias para interpretar ou confirmar dados obtidos por meios tecnológicos.



-Tecnológico: é obtido através da análise e interpretação de informações obtidas em sistemas eletrônicos, bem como da interceptação e descriptografia de transmissão de informações por qualquer meio eletrônico.

REGRA

REGRA

4.4 POR SUA ATIVIDADE

- **Política:** é o conhecimento das capacidades potenciais e atuais dos atores que podem ou geram riscos no nível político. também o estudo dos fatores estruturais que explicam as características do sistema político do Estado.

- **Económico:** é o conhecimento das capacidades potenciais e atuais dos atores que podem ou geram riscos a nível económico. Seu principal objetivo é detectar distorções ou manobras que possam afetar os interesses da nação.

REGRA

- **Social:** é o conhecimento das capacidades atuais e potenciais dos atores que geram ou podem gerar riscos no nível social. Isto é obtido através da análise dos actores, da organização e do comportamento dos fenómenos sociais que podem afectar e intervir no bem-estar da governação e/ou da ordem constitucional.

- **Nacional:** conhecimento útil para a formulação e execução da política geral do governo, fornecido ao Presidente Constitucional da República e ao Conselho de Ministros, com o objetivo de garantir a vigência dos direitos humanos.

REGRA

- Militar: é o conhecimento das capacidades e vulnerabilidades do poder e potencial dos atores que geram ou podem gerar riscos no campo militar, que serve para garantir a independência, a soberania, a integridade territorial e a ordem constitucional.

- Polícia: é o conhecimento das capacidades e vulnerabilidades dos atores nacionais e/ou estrangeiros que geram ou podem gerar riscos no campo militar.

CAPÍTULO V

PROCESSO INTELIGÊNCIA (PI)

Inclui a orientação do esforço de busca, a busca e análise de informações, principalmente informações de fonte fechada, isso significa que essas informações são secretas, o produto final é uma inteligência que é organizada para uso em atividades como campanhas eleitorais e/ou governamentais.
Antes do processo de inteligência, é fundamental ter em conta os objetivos e cenários de risco que possam ser estabelecidos, bem como os recursos disponíveis para cumprir esse objetivo.

Para atingir o objetivo, o processo de inteligência inclui as seguintes fases:

Fuente: DINI

Entre a fase de Processamento da Informação e a Orientação do Esforço de Busca, a hipótese pode ser reorientada sempre que a informação requerida assim o exigir, iniciando-se assim um novo cenário de risco e consequentemente gerando novas necessidades de informação.

5.1 PRIMEIRA FASE: Orientação do esforço de busca

É o conjunto de ações que se realizam de forma permanente com o objetivo de direcionar as capacidades de busca para os objetivos do nosso candidato e/ou partido político.

Segundo a DINI, nesta primeira fase deverão ser seguidas as seguintes etapas:

a) Comunicação de necessidades de inteligência

Nesta fase, os analistas dos órgãos de inteligência recebem o que é necessário para compreender as informações dos níveis

superiores.

b) Determinação de indicações

Uma indicação é uma indicação, evidência ou característica do ator e do ambiente, que sustenta uma presunção sobre os fatos, fenômenos, situações, comportamentos, vulnerabilidades, possibilidades e formas de ação.

c) Determinação da prioridade da necessidade de inteligência.

Nesta fase, a inteligência é recebida e analisada para estabelecer variáveis de informação, que são então classificadas por ordem de prioridade, destacando os elementos de informação essenciais e outras necessidades de informação.

Permitindo assim a utilização de órgãos de busca de forma mais eficiente e eficaz.

Os elementos essenciais da informação são as variáveis prioritárias ou lacunas de informação, formuladas sob a forma de questões que, se não forem respondidas, impedem a concretização dos objectivos previamente estabelecidos.

A informação de segunda prioridade dificulta a consecução dos objectivos.

d) Determinação das bases para pedidos

Estas são as informações específicas que foram solicitadas para responder aos elementos essenciais de informação e às demais necessidades de informação levantadas.

e) Determinação dos órgãos

É a seleção dos órgãos de busca mais adequados para cada situação e informação necessária, que serão ordenados para realizar a busca de informação na qual são levados em consideração os seguintes fatores:

- **Acesso:** inclui levar em consideração o nível de renda e sem restrições que o órgão de busca tenha quanto à fonte da informação.

- **Possibilidade:** Os órgãos de busca devem ser fisicamente capazes de obter as informações desejadas.
- **Adaptabilidade: deverão** ser utilizados os órgãos mais adequados para a obtenção das informações desejadas, levando em consideração os aspectos pessoais, econômicos e materiais.
- **Multiplicidade:** para obter as informações solicitadas é necessário utilizar mais de um órgão de busca, para que as informações obtidas pelos diversos órgãos possam ser comparadas.
- **Equilíbrio:** é a racionalidade do trabalho de forma equitativa entre os órgãos de busca disponíveis.
- **Localização:** consiste em levar em consideração a proximidade do órgão em relação à fonte de informação.

f) Formulação de pedidos de informação

Dentro do sistema nacional de inteligência é um documento dirigido a qualquer órgão de inteligência, para que forneça informações específicas.

g) Coordenação e supervisão permanentes

É o acompanhamento e monitoramento dos órgãos de busca, incluindo a análise de resultados parciais ou finais, com a finalidade de realizar os reajustes e modificações necessárias no processo de busca de informações.

5.2 SEGUNDA FASE: Busca de informações

É o processo de execução de atividades destinadas a L A obtenção de informações é realizada por meio da exploração sistemática e ordenada das fontes com meios e técnicas operacionais para posterior entrega ao órgão superior.

Esta segunda fase possui características que devem ser levadas em consideração:

- **Previsão: os eventos** devem ser antecipados; isso requer planejamento detalhado e execução oportuna de ações de busca.
- **Permanência:** a necessidade de ter inteligência em todos os momentos exerce um esforço contínuo ao longo do tempo para buscar informações.
- **Dinâmico:** a busca de informações deve ser realizada com iniciativa e decisão, dependendo da dinâmica dos acontecimentos.

- **Reserva:** esta característica é muito importante e deve ser levada em consideração, pois a busca de informações só deve ser conhecida e divulgada entre pessoas autorizadas.

Nesta fase de procura de informação, é importante determinar ou saber quais são as nossas fontes de informação, pois são todas aquelas pessoas, organizações, comunicações, infra-estruturas, actividades ou locais onde se pode obter informação útil.
As fontes de informação são classificadas por:

- Pela sua importância:

a) Fonte fechada

É aquele que contém a informação necessária mas está protegida, pelo que é necessário realizar atividades de infiltração para acessá-la e obtê-la.

b) Código aberto

Acesso limitado: são aqueles administrados por órgãos públicos ou privados. Por exemplo, sigilo bancário, sigilo fiscal, etc.

Acesso ilimitado: é aquele que está disponível gratuitamente e oferece informações não classificadas. Por exemplo, as atividades públicas dos nossos adversários políticos, entre outras.

A classificação também se baseia na sua **origem** e isso foi explicado - anteriormente.

· Etapas de busca de informações

a) Planejamento

Consiste na determinação das fontes, órgãos e procedimentos a serem utilizados na coleta.

REGRA

b) Coleção

Consiste no conjunto de atividades que se orientam à exploração de fontes para atingir o objetivo. É aqui que a fonte é explorada, organizada e analisada.

c) Formulação da nota do agente

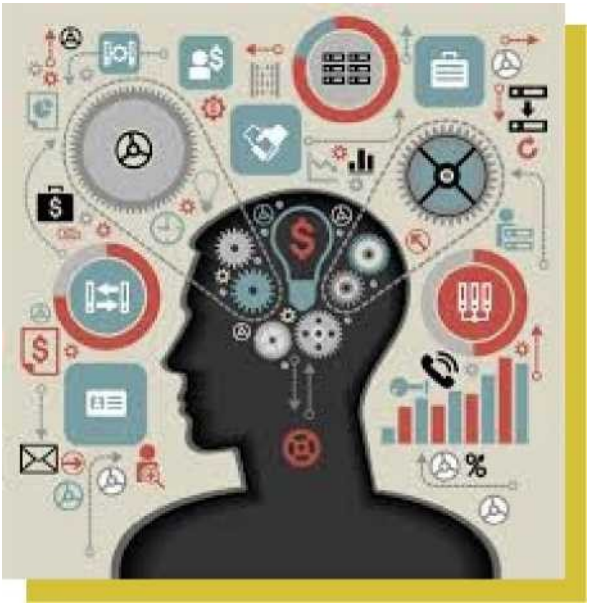
É o documento elaborado pelos órgãos de busca no qual a informação deve responder às seguintes questões: o quê, quem, quando, onde e como, em relação à missão da informação a ser obtida.

d) Distribuição das informações obtidas

Consiste em transmitir de forma objetiva as informações obtidas e avaliadas pelo órgão de busca da organização.

5.3 TERCEIRA FASE: Processamento de informações

Consiste na exploração da informação obtida, através do seu registo, avaliação, análise e conclusão. Transformá-lo em um produto de inteligência com alto grau de certeza e previsão.



5.4 QUARTA FASE: Disseminação e uso de inteligência

Consiste na entrega do produto de inteligência aos usuários autorizados, de forma oportuna, adequada e sobretudo por meio de canal seguro.

Este procedimento é em relação à sua importância, natureza, meios disponíveis, nível de produção corporal, entre outros.

CAPÍTULO VI

ESPIONAGEM ELEITORAL

A implementação deste tipo de ferramentas nas campanhas eleitorais exige um forte investimento, lealdade, disciplina e, acima de tudo, experiência. Esta estratégia deve ser utilizada com discrição, por isso é importante fingir que ela não existe, e não é necessário que todos os membros da Sala de Guerra da campanha eleitoral a conheçam.

O uso de inteligência e contrainteligência é comum em campanhas eleitorais em vários países, muitas vezes passa despercebido já que as equipes de campanha permanecem cautelosas com o caso, porém se for descoberto as consequências são graves tanto para o partido político quanto para o candidato.

Principalmente para obtê-la se utiliza inteligência humana e cibernética, a seguir mostramos instrumentos que são e podem ser utilizados na espionagem política, isso obviamente com a ajuda de um infiltrado, seja de forma consciente ou inocente.

6.1 ARTIGOS DE ESPIONAGEM

· **USBs espiões profissionais - Com câmera e gravador ocultos** Os USBs espiões, que incluem câmeras espiãs de vídeo e/ou gravadores de voz integrados, são uma das maneiras mais eficazes de contornar medidas e sistemas de segurança. Por ser um objeto pequeno e muito comum, ninguém se surpreenderia se você carregasse o USB em reuniões, no trabalho, em casa, com amigos ou em qualquer situação. Além disso, graças ao seu tamanho podemos adicioná-lo ao nosso porta-chaves e será muito mais fácil camuflá-lo e deixá-lo sobre a mesa ou outro local.

A câmera USB é muito útil em negociações, reuniões de planejamento estratégico, ataques ou outras ações que possam nos ajudar com o adversário político.

Existem dois tipos de espião USB; aquele com o qual você pode gravar vídeo, tirar fotos e áudio e aqueles que são apenas um gravador digital para gravar qualquer tipo de conversa ambiental, até mesmo conversas telefônicas.

· **MICROFONES ESPIÕES**

Microfones são dispositivos projetados para gravar e modular som. Possui alto grau de adaptabilidade tanto no âmbito recreativo quanto no profissional, podendo encontrar rádios, talk centers ou no mundo da espionagem. Atualmente existem vários tipos de microfones com diferentes utilizações e cada um tem características próprias dependendo de como serão utilizados. Alguns deles que consideramos úteis na espionagem são os seguintes:

· **Microfones telefônicos ou elétricos**

Este tipo é um poderoso transmissor que é instalado em qualquer lugar da linha telefônica que envia todas as conversas realizadas através do aparelho telefônico para o receptor, que capta o som e pode ser gravado. É pequeno e não necessita de bateria, pois é alimentado diretamente pela tensão da rede telefônica. A maior gama de ação desses dispositivos é a espionagem realizada pelas forças de segurança e como microfone espião secreto.

· **Microfone GSM**

O funcionamento do microfone GSM é o mesmo que podemos ver nos telemóveis, bastando inserir um cartão SIM ao qual nos conectaremos.

Podemos ouvi-lo remotamente e até gravá-lo. Depois disso, nos conectaremos usando um sinal wireless que ligará nosso microfone. A partir desse momento estará operacional e poderá realizar coleta de áudio por horas. Sua bateria é variável de acordo com as características de cada aparelho.

Nos últimos anos, a técnica dos microfones espiões foi aperfeiçoada, inserindo-os em objetos que, ao mesmo tempo que os camuflam, proporcionam-lhes autonomia ilimitada. Vemos um exemplo disso em sua ocultação em utensílios como réguas de energia que serão conectadas diretamente na tomada. O que sem dúvida já não é limitado é o alcance do sinal, pois se trata de uma ligação global, podendo ser activada a partir de qualquer ponto do planeta com um simples telefonema.

· óculos de espionagem

Os óculos espiões com câmera escondida são um dos objetos do cotidiano mais utilizados na espionagem e no registro de imagens feitas com câmera escondida.

Existem muitos modelos de óculos e muitos usos para eles. Um uso

muito comum entre os alunos é o uso de óculos espiões para exames, embora possam ser usados em reuniões de trabalho e em qualquer outra situação do dia a dia.

Podemos encontrar modelos de óculos espiões para homem e mulher, e os avanços da tecnologia permitem-nos encontrar os melhores óculos espiões da atualidade por menos de 100€. Os melhores modelos permitem gravar em alta definição.

Além disso, todos os modelos vêm com instruções para óculos espiões e são modelos atuais para que possam se passar por lentes normais.

· **Chaveiro espião com câmera escondida**

Os chaveiros são um dos objetos do cotidiano menos suspeitos e que passam despercebidos pelas pessoas, já que a maioria de nós tem um (pelo menos) onde carregamos as chaves de casa, do trabalho ou do carro (em um chaveiro especial).

O facto de serem tão comuns e de não nos surpreendermos com a sua presença torna-os objectos ideais para espionagem. Neste artigo vamos apresentar diversos modelos diferentes de chaveiros espiões e

suas características técnicas.
Uma característica comum a todos eles é que possuem uma câmera escondida e um microfone espião para fazer gravações sem levantar suspeitas.

· **relógio espião com câmera escondida**
Um relógio espião é um relógio funcional que incorpora elementos de espionagem. No caso dos relógios, possuem câmeras ocultas, com funcionalidades dependendo do modelo, pois podem ser relógios de pulso masculinos ou femininos, relógios de parede com câmera camuflada. relógio com câmera espiã (analógica ou digital ou qualquer tipo de relógio).
As câmeras que incorporam também variam em suas características dependendo das funções a que se destinam. Os despertadores costumam ter câmera com visão noturna, alguns são HD (alta definição), também achamos resistentes à água.


Cámara oculta
Micrófono

CAPÍTULO VII

ANÁLISE DE CASO

7.1 LOURDES FLORESNANO 2010, PERU

No âmbito de uma campanha negra, utilizando inteligência tecnológica, interceptaram os telefonemas da então candidata, Lourdes Flores Nano, onde ela demonstrou seu aborrecimento e comentários sobre os resultados das pesquisas e quando foram divulgados pela mídia, afetaram o a sua reputação e a sua aceitação junto dos eleitores, portanto, para evitar este tipo de ações, é necessária a contra-espionagem e evitar este tipo de atos.

Áudio: https://www.youtube.com/watch?v=z9zuKs9wLQo

7.2 HILLARY CLINTON 2016

Nas eleições presidenciais dos Estados Unidos, o Wikileaks vazou os e-mails da campanha de Hillary Clinton. Estes e-mails perturbaram as eleições presidenciais de 2016, onde o FBI encontrou quase 15.000 e-mails a mais do que Clinton alegou ter entregue às autoridades. Esses foram os motivos da polêmica e, portanto, do escândalo.
O email que Hillary utilizou não foi o que lhe foi fornecido pelo Estado, mas sim através de uma conta pessoal quando ainda era Secretária de Estado.

7.3
ANDRÉSSEPÚLVEDA (COLÔMBIA)

Sepúlveda é um dos hackers mais conhecidos devido à sua carreira iniciada em 2005, e seus primeiros trabalhos foram menores, consistindo principalmente em modificar sites de campanha e violar bancos de dados da oposição com informações sobre seus doadores.
Ao longo dos anos, ele reuniu equipes que espionaram, roubaram e difamaram campanhas presidenciais na América Latina. Numa manifestação Sepúlveda diz que instalou um vírus nos routers da sede do PRD. E então ele grampeou telefones e computadores e roubou estratégias de campanha. Ele conhecia os discursos de seus rivais - enquanto os editores os escreviam. Da mesma forma, gerenciei milhares de contas falsas em redes sociais e as utilizei para direcionar a “conversa” dos usuários para os planos que Peña Nieto promovia. Sepúlveda tinha um orçamento muito elevado para realizar estas ações.


Bloomberg
Businessweek
CONFESSIONS
OF
A
One man's
story of
manipulating
elections across
Latin America
POLITICAL
HACKER

CAPÍTULO VIII

PROCESSO CONTRAINTELIGÊNCIA

São um conjunto de atividades cujo objetivo fundamental é neutralizar as capacidades e operações de inteligência.
Para evitar atos de espionagem e sabotagem como mostra a análise do caso, é necessário tomar precauções e prevenir atos hostis.
O processo de contrainteligência toma produtos de inteligência como insumos para produzir e aplicar medidas de contrainteligência, que são divididas da seguinte forma:

8.1 CONTRA-INTELIGÊNCIA PASSIVA

São um conjunto de atividades sistemáticas, permanentes e preventivas, cujo principal objetivo é identificar vulnerabilidades da nossa equipe para evitar infiltração e/ou exploração por inteligência hostil, onde devem ser seguidas as seguintes fases.

Análise e avaliação de riscos
São ações que estudam e correlacionam variáveis como ameaças,

vulnerabilidades e impactos para obter os correspondentes níveis de risco, bem como as possíveis repercussões pela sua incapacitação ou destruição, utilizando normas e padrões nacionais e internacionais. Num equipamento deve ser sempre realizado o correspondente estudo de segurança, que inclui a análise das variáveis acima mencionadas (análise de risco). Esta fase destina-se a orientar a execução de medidas passivas de contra-espionagem.

57

Resposta ao risco

Consiste na aplicação de medidas passivas de contrainteligência com o objetivo de mitigar as vulnerabilidades detectadas e/ou minimizar ou eliminar o impacto em caso de ato hostil. Para tanto, é formulado um plano permanente.

Supervisão e controle

Consiste num conjunto de ações realizadas periodicamente na administração da nossa equipa, com o objetivo de verificar o nível de cumprimento das suas normas técnicas na aplicação das medidas passivas estabelecidas. É conveniente considerar que nenhuma medida de segurança será suficiente, pelo que é necessária uma - estimativa constante da análise e gestão de riscos com base nas novas informações disponíveis (ciclo de melhoria contínua) para atualizar as medidas passivas de contrainteligência.

8.2 CONTRA-INTELIGÊNCIA ATIVA

Consiste num conjunto de atividades que são realizadas direta e ofensivamente contra um ator para neutralizar as suas formas de ação ou capacidades de inteligência, que ameaçam ou podem ameaçar o nosso partido político e/ou candidato. Materializa-se através da aplicação de medidas activas no âmbito da contra-espionagem, contra-sabotagem, contra-subversão e outras actividades encobertas.

A contrainteligência ativa inclui as seguintes fases:

· **Planejamento de medidas ativas**

A partir da análise das capacidades, vulnerabilidades e formas de atuação da estrutura clandestina de um determinado ator, são estabelecidas as medidas ativas que serão executadas para neutralizá-la. O plano de operações deve conter uma síntese da situação, missão, conjunto de medidas, programa de aplicação (forma e calendário), órgãos e equipas empenhados.

· **Intervenção**

Atuar direta e ofensivamente sobre o ator de uma ameaça com o objetivo de eliminar sua capacidade de executar atos hostis ou neutralizar suas formas de atuação em curso. Às vezes a intervenção não será realizada diretamente pelo órgão de contra-espionagem, mas

sim por aqueles considerados mais pertinentes.

· **Avaliação e reporte de resultados**

Ao final da operação, a equipe de contrainteligência deverá avaliar os resultados alcançados em relação aos objetivos estabelecidos. Deve ser preparado um relatório que contenha uma descrição da atividade hostil detectada e as ações tomadas para neutralizá-la.

CAPÍTULO IX

MEDIDAS DE CONTRAINTELIGÊNCIA

É o conjunto de ações e disposições adaptadas para proteger informações secretas contra atividades de inteligência hostis, através da execução de contra-infiltração, contra-espionagem, contra-sabotagem, contra-subversão e outras atividades encobertas. Estas medidas também incluem a segurança cibernética.
É importante ter em mente que o nosso adversário aproveitará todas as nossas vulnerabilidades para aumentar a sua capacidade e impedir o cumprimento dos nossos objetivos.
Eles são classificados da seguinte forma:

Processo de contrainteligência	
Contrainteligência Passiva	**Contrainteligência Ativa**
Análise e avaliação de risco **Resposta ao risco** **Supervisão e controle**	**Planejamento de medidas ativas** **Intervenção** **Avaliação e reporte de resultados**

9.1 MEDIDAS PASSIVAS

São aquelas disposições e procedimentos de natureza socialmente defensiva, produto da contrainteligência passiva, que servem para proteger a informação do nosso partido e/ou candidato, controlando as vulnerabilidades que apresentam.
São chamados de passivos, porque são aplicados controles e medidas ao pessoal e aos recursos próprios para neutralizar ou mitigar o impacto de uma ação hostil. Algumas das medidas passivas são de amplo espectro, pois podem prevenir ou minimizar mais de um tipo de

risco.

Alguns dos recursos são:

1. Sua aplicação é generalizada.
2. Sua natureza é defensiva e permanente.
3. Aplicam-se a pessoal e recursos próprios.
4. São de amplo espectro porque podem prevenir ou neutralizar mais de um tipo de atividade hostil.

9.2 MEDIDAS ATIVAS

São de natureza ofensiva e são aplicados no âmbito da contra-espionagem. É realizado por meio de intenso trabalho de detecção, avaliação e identificação de atividades de inteligência hostil.

Enquanto medidas passivas são aplicadas às vulnerabilidades das nossas informações secretas, medidas ativas são aplicadas a um ator de ameaça que procura afetar as suas capacidades e formas de ação, previamente detectadas e avaliadas, a fim de neutralizar qualquer ação hostil potencial ou em curso. nossos oponentes.

As medidas ativas, diferentemente das passivas, são específicas, ou seja, visam neutralizar uma ação hostil específica (infiltração, espionagem, sabotagem, subversão e outras atividades encobertas).

9.3 MEDIDAS DE ENGANO

São as ações que se aplicam indistintamente na contrainteligência ativa e/ou passiva, com o objetivo de alterar a percepção de um ator e disponibilizar a execução de suas ações a fim de neutralizá-las. Recorrem à mentira, à astúcia, à malandragem, para induzi-lo e mantê-lo no erro. Isso significa que, ao tomar conhecimento das atividades de inteligência do adversário, você receberá informações falsas para que possa repassá-las à sua equipe.

As duas partes básicas de uma manobra de engano são:

1) Dissimulação: consiste em esconder o que é real.
2) Simulação: é mostrar o falso como real.

Todas as ações de engano têm como objetivo desinformar. Desinformação é qualquer comunicação ou manifestação aberta ou encoberta que contenha material intencionalmente falso e/ou enganoso. Muitas vezes é combinada seletivamente com informações verdadeiras, buscando enganar ou manipular, com o objetivo de criar convicção quanto à veracidade do material apresentado e, consequentemente, predispor o ator a realizar ações de acordo com os interesses de quem espalha a desinformação .

9.4 ATIVIDADES SECRETAS CONTRA A SEGURANÇA DE NOSSAS INFORMAÇÕES SECRETAS

São aquelas atividades que um ator realiza para afetar a disponibilidade, integridade e/ou confidencialidade de nossas informações mais secretas.

As atividades secretas contra a segurança de nossas informações secretas são classificadas como:

- **Infiltração:** conjunto de atividades para atingir a penetração de objetivos e interesses, com a finalidade de realizar espionagem, sabotagem, subversão ou outras atividades encobertas.
- **Espionagem:** conjunto de atividades para obter clandestinamente nossas informações classificadas, cujo - conhecimento constitui um valioso elemento de julgamento para decisões que ameacem nossas informações secretas. A espionagem pode ser humana e cibernética. Portanto, é importante tomar precauções e evitar o vazamento de informações que possam nos afetar.

REGRA

- Sabotagem: conjunto de atividades para interferir, impedir ou dificultar o alcance de nossos objetivos. A sabotagem pode ocorrer devido aos dados que nosso oponente possui ou devido a algum elemento importante para nossa organização, partido político e/ou candidato. Por exemplo, conhecimento de alguma atividade a ser realizada pelo nosso candidato.

- Subversão: Conjunto de atividades clandestinas para organizar e/ou promover ações que buscam minar a autoridade legitimamente constituída, ignorá-la e/ou alterar a ordem estabelecida. Isto pode ser feito numa campanha eleitoral quando adversários organizados aparecem num comício e/ou aparição pública do nosso candidato.

9.5 OPERAÇÕES DE CONTRAINTELIGÊNCIA

São aquelas atividades de natureza secreta que servem para atingir objetivos específicos de contrainteligência. Inclui ações de detecção, investigação, identificação e intervenção. São realizadas por pessoal especializado e visam neutralizar as atividades e capacidades dos atores hostis em termos de infiltração, espionagem, sabotagem, subversão e outras ações encobertas.

As operações de contrainteligência procuram detectar operações de inteligência hostis e, portanto, agir diretamente sobre a ameaça. É classificado da seguinte forma:

Operações de monitoramento: São desenvolvidas permanentemente para detectar indícios ou fatos sobre atividades secretas contra nossas informações classificadas. Incluem ações de detecção, investigação e identificação que servem para adotar as medidas de contra-espionagem mais adequadas e assim prevenir qualquer tentativa de infiltração hostil. As operações de monitoramento também são conhecidas como operações de controle.

Operações de intervenção: são executadas a partir da detecção da operação de inteligência do nosso oponente e/ou adversário, têm como finalidade prevenir ou neutralizar qualquer ação em

execução ou capacidade em desenvolvimento que represente um risco aos nossos objetivos.
Eles são classificados da seguinte forma:

- Contra-espionagem: Tem como objetivo prevenir ou - neutralizar uma operação de inteligência humana ou técnica destinada a obter informações confidenciais sobre os nossos dados confidenciais. Simultaneamente, a operação de contraespionagem cria a oportunidade de reunir informações sobre o agente da espionagem.

- Contra-sabotagem: visa prevenir ou neutralizar operações de sabotagem sobre nossas informações classificadas. É complementado pela contra-espionagem, uma vez que visa bloquear os esforços de informação do sabotador para obter informações sobre os nossos activos críticos.

Contrasubversão: visa prevenir ou neutralizar operações de inteligência destinadas a organizar e/ou promover movimentos subversivos.

Contra outras atividades encobertas: tem como objetivo prevenir ou neutralizar qualquer outra forma de ação hostil de inteligência.

Consequentemente, é importante ter em conta a importância da contra-espionagem para que desta forma o adversário não tenha acesso aos nossos dados confidenciais, mas como evitar a espionagem Isto é feito através de uma estratégia mas é importante saber quais são os instrumentos? são com os quais podemos combater a espionagem.

CAPÍTULO X

ARTIGO DE CONTRAINTELIGÊNCIA

10.1
CÂMERAS ESPIÕES E DETECTORES DE MICROSCÓPIO

Existem diferentes detectores de câmeras espiãs no mercado que nos ajudam a localizar facilmente onde esses pequenos dispositivos estão escondidos; para neutralizar tentativas de espionagem. Isso nos ajudará a evitar sermos gravados e espionar qualquer informação - secreta.

· **Detector de câmera sem fio:**

É um aparelho especialmente desenvolvido para saber se há minicâmeras te observando. Alguns também podem ser utilizados como detectores de frequência, sendo assim um dispositivo que se adapta a diversos tipos de necessidades.

· **Detectores de eletrodomésticos ocultos:**
Especializou-se na busca de dispositivos colocados por terceiros.

REGRA

10.2 DETECTORES NÃO LINEARES

Encontra dispositivos eletrônicos que contenham elementos semicondutores (gravadores de áudio, microfones, dispositivos de rastreamento, etc.) mesmo quando os dispositivos estão desconectados e desligados, exibindo os níveis de detecção em um painel de LED.

A aplicação da faixa de micro-ondas oferece oportunidades únicas para detectar elementos semicondutores ocultos por diferentes materiais, detectando através de rachaduras, paredes desenterradas, reflexos de superfícies lisas.

74

10.3 DISRUPTORES DE MICROFONE

Ele foi projetado para proteger conversas e evitar vazamentos de informações. Foi criado a partir de conversas reais entre pessoas e o resultado é semelhante ao barulho de uma multidão conversando em um espaço público movimentado. As conversas misturam vozes masculinas e femininas em inglês, gerando uma fala absolutamente ininteligível.

O ruído que gera cria uma barreira adicional que interfere e mascara a fala, garantindo que nada nem ninguém possa burlar a confidencialidade.

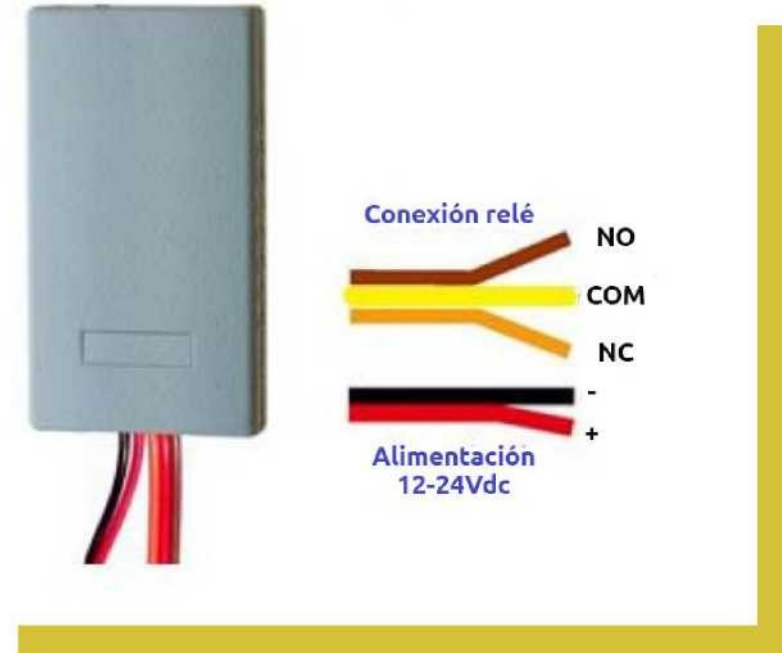
O gerador evita que as conversas sejam capturadas por gravadores de voz espiões, microfones espiões GSM, microfones com fio, câmeras espiãs ou qualquer dispositivo de vigilância.

10.4 DETECTORES INIBIDORES DE FREQUÊNCIA

O que os bloqueadores de frequência fazem é saturar a largura de

banda das comunicações em um determinado raio.

Para isso eles obviamente precisam emitir um sinal muito forte que nada mais é do que um ruído branco que dificulta, e de fato impede, que o resto dos sinais ao seu redor possam se comunicar.



10.5 SEGURANÇA CIBERNÉTICA

· Criptografar mensagens e conteúdo

Uma das melhores maneiras de proteger as informações é criptografá-las. Embora não garanta que outras pessoas possam acessar as mensagens e o conteúdo, pelo menos os força a encontrar um método para descriptografá-los. Entre os aplicativos mais populares para estabelecer comunicações seguras estão Silent Circle, Cryptocat, Red Phone e SeeCrypt. Isso evita que eles acessem informações confidenciais de nossa equipe de -campanha e/ou candidato.

· Proteção contra vírus e trojans

A tecnologia avança em grande velocidade, mas também as técnicas dos cibercriminosos, que geram todos os dias novas

ameaças projetadas para todos os tipos de dispositivos. Por este motivo, é aconselhável manter o seu computador e smartphone protegidos com algum tipo de antivírus que detecte e neutralize ataques de Trojan e outros tipos de software malicioso. Para impedir o acesso aos nossos dados.

· **Alterar sistema operacional móvel**

Sistemas operacionais como Windows e Mac OS, por serem os mais populares e utilizados, são também os mais expostos à ciberespionagem. As alternativas minoritárias, baseadas em Linux e com a mesma filosofia de software livre e código aberto, são as que oferecem maior segurança. Entre os sistemas operacionais mais recomendados estão Debian, Gentoo, Linux Mint e Fedora.


debian
GNU/Linux

· Adeus ao Google

Hoje em dia dá para viver sem consultar o Google? Você pode, embora o Bing e o Yahoo! As pesquisas não são boas - alternativas se o que se procura é proteger ao máximo a privacidade das informações classificadas, uma vez que também pertencem a grandes empresas e registam a navegação dos utilizadores. O mecanismo de busca que mais respeita a privacidade do usuário é o DuckDuckGo. Esta filosofia de confidencialidade é compartilhada pela Startpage (que oferece resultados do Google atuando como intermediário), ixquick e MetaGer. Já o Ask.com, o maior entre os pequenos buscadores, oferece a possibilidade de navegar sem ser rastreado.

E-mail alternativo

Embora as mensagens instantâneas e os smartphones tenham mudado a forma como nos comunicamos, o e-mail não perdeu força e continua sendo um dos serviços online mais utilizados no mundo.

Você pode comprar os e-mails mais seguros em:

- ProtonMail: Um sistema de e-mail criptografado de ponta a ponta com sede na Suíça. Fa-

fácil de usar, de código aberto e permitindo criar um e-mail anônimo sem precisar fornecer seus dados. Seu site oficial é Protonmail.com/es.

- **CounterMail:** é um serviço com e-mails criptografados ponta a ponta e cabeçalhos anônimos, que você pode levar para qualquer lugar e é compatível com todos os sistemas operacionais desktop e Android. Tudo isso também focando na facilidade de uso. Seu site oficial é Countermail.com

- **Posteo:** Com um preço surpreendentemente barato, o Posteo posiciona-se como uma alternativa a considerar. Possui criptografia ponta a ponta que você pode configurar em clientes de terceiros e a capacidade de criar uma agenda de contatos criptografada. Seu site oficial é Posteo.de.

- **Hushmail:** Serviço voltado para usuários inexperientes que possui cliente web e aplicativo oficial para iOS. Com múltiplas camadas de segurança e criptografia ponta a ponta, sem publicidade e aliases de e-mail ilimitados. Seu site oficial é Hushmail.com.

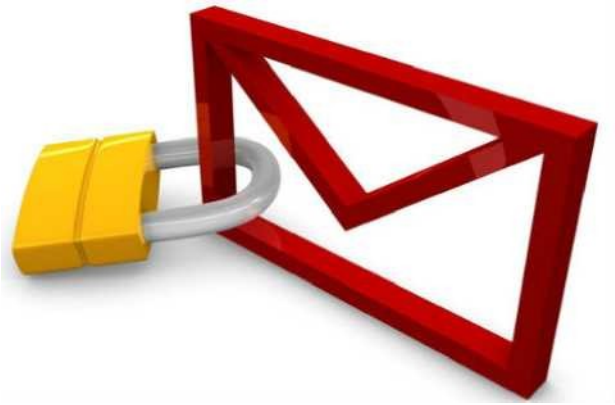
- **Mail Fence:** Um serviço sem rastreamento e sem anúncios com calendário, documentos, garantia de chave e criptografia de ponta a ponta. Seu registro não é anônimo, mas você pode escolher seus domínios e utilizá-los em aplicativos desktop, Android e iOS. Seu site oficial é Mail-fence.com.

- **Tutanota:** Protege com criptografia ponta a ponta e 2FA, e possui aplicativos oficiais para Android e iOS para que você possa levá-lo sempre com você. É vendido como uma alternativa ao Gmail com um ambicioso plano gratuito e webmail. Seu site oficial é Tutanota.com/es.

- **Runbox:** Além de ser outro serviço importante para criar

seu e-mail anônimo, eles ganham a medalha de serem verdes ao obterem energia de usinas hidrelétricas renováveis. Não oferece uma conta gratuita como as outras da lista, mas possui até quatro planos de pagamento diferentes. Seu site oficial é Runbox.com.

- **Caixa postal:** Com mais de 20 anos de experiência, é um dos clássicos do setor. Oferece seu próprio cliente web para que você possa utilizá-lo de qualquer lugar e oferece complementos como agenda, calendário e gerenciador de tarefas. Possui uma conta simples e barata para usuários, mas também outros planos mais avançados para grupos e empresas. Seu site oficial é Mailbox.org.



· **Mergulhe na Internet incógnito**

Chrome, Firefox, Internet Explorer e Safari compartilham o mercado na área de navegadores e todos eles já foram suspeitos de coletar dados de usuários para fins comerciais. Além disso, essas informações também podem cair em outras mãos por meio de ordem judicial que assim o exija.

Para evitar esse rastreamento, todos esses navegadores - possuem sistemas que permitem navegar incógnito, por isso é aconselhável utilizá-los. Outra possibilidade é utilizar o programa DoNotTrackMe, que protege o internauta de qualquer aplicativo espião escondido na web.

· **Um navegador diferente**

Para quem não confia nos sistemas anti-rastreamento dos grandes navegadores, existem opções focadas na privacidade do usuário como Dooble, Omniweb (como alternativa ao navegador Mac), SRWare Iron, Tor e JonDonym.

· **Apague o rastro**

Ao terminar de usar o computador, é uma boa ideia apagar qualquer vestígio que possa ter ficado se você não tiver tomado cuidado

suficiente antes. No Windows, esta opção encontra-se no famoso “Painel de Controle, Opções da Internet”. Mas, além disso, geralmente é conveniente excluir também os dados do navegador que foi usado. O histórico deve ser apagado, mas também formulários, senhas, cookies e arquivos temporários.

· **Redes sociais menos conhecidas**

Na escolha das redes sociais surge um problema adicional que outros serviços online não têm: é necessário que outras pessoas (familiares, amigos, conhecidos) as utilizem para que tenham alguma utilidade. Entre as redes minoritárias, as opções não são escassas: Buddycloud, Diaspora, Friendica, Movim, pump.io, GNU Social, telegram, entre outras. O que permite maior segurança para poder planejar algo por meio de mensagens criptografadas de ponta a ponta.

· Senhas seguras

Embora esta recomendação conste de todos os guias de navegação segura, ainda são muitos os utilizadores que recorrem a palavras-passe tão fracas como “123456”, “abc123”, “111111”, “qwerty” ou “Parliament 2020”. É aconselhável utilizar senhas “fortes”, ou seja, aquelas que combinam letras maiúsculas e minúsculas, além de números e sinais de pontuação. Além disso, não é bom usar a mesma senha para todas as contas e nem, claro, salvá-las em computadores públicos.

· Impressões digitais?

Além das senhas, dos pins numéricos e dos padrões de desbloqueio, os sistemas de segurança biométrica, como o reconhecimento facial ou as impressões digitais, estão gradualmente proliferando, muitos dispositivos contam atualmente com essa medida de segurança.

Evite fontes não confiáveis

Uma dica que parece óbvia, mas que ainda é preciso lembrar de vez em quando. Você nunca deve abrir arquivos ou links enviados por estranhos, seja em redes sociais, e-mail ou serviços de mensagens instantâneas. Você nunca deve instalar um aplicativo para o qual não tenha referências ou que não ofereça total confiança. Você também deve ter cuidado ao fornecer os dados do seu banco ou cartão de crédito, isso só deve ser feito em sites confiáveis, caso contrário eles poderão acessar os dados de nossas operadoras e celulares.

REGRA

CONCLUSÕES

Com o passar dos anos, a espionagem tornou-se mais profissional, passando do campo militar para outras áreas, como a política. Por isso, as técnicas militares são adaptadas ao campo da política para seu melhor aproveitamento e eficácia. Muitos partidos contratam especialistas para realizar atos de espionagem contra o adversário político e utilizam os materiais mencionados neste e-book para obter dados secretos e assim derrotar o adversário político.

O processo de inteligência utilizado possui um método que deve ser seguido para obter os dados exigidos do oponente. Da mesma forma, o processo de contrainteligência é essencial para detectar atos hostis ao nosso candidato, organização e/ou partido político e assim proteger os nossos dados confidenciais.

RECOMENDAÇÕES

1. Tenha uma estratégia: é preciso levar em conta que um processo de inteligência tem um objetivo, mas esse objetivo tem que estar de acordo com a estratégia que foi estabelecida.

2. Trabalhe com profissionais: é importante ter em mente que os atos de inteligência e contrainteligência devem ser realizados entre pessoas de alta confiança e onde prevalece a lealdade para que os planos não sejam divulgados.

3. Organize sua equipe: ter uma equipe organizada onde cada um conheça as funções e as desempenhe é muito importante para que ela seja reprodutível e eficaz.

4. Proteja suas informações: a única forma de proteger suas - informações é através da prevenção e da contrainteligência nas quais devem ser detectados atos hostis e tomadas medidas contra esses atos.

5. Utilize materiais tecnológicos: não só para espionagem, mas também para se proteger contra esses atos e assim evitar a divulgação de suas informações sigilosas.

LITERATURA

1. Sherman Kent “inteligência estratégica” 1949 Kent, Sherman. (1978).

2. Direcção Nacional de Inteligência. 2013

3. PlattWashington 1974. A produção de inteligência estratégica. tradução de Álvaro Galvão Pareira e Capitão Heitor Aquino Ferreira. Rio de Janeiro. Biblioteca do Exército; Livraria editora interina.

4. Karl Von Clausewitz “Da Guerra”.1832

5. Sun Tzu (2003). A arte da guerra: biblioteca virtual universal. (Escrito aproximadamente no século V.)
Obtido em: https://www.biblioteca.org.ar/libros/656228.pdf

6. Navarro Bonilla, Diego. O ciclo de Inteligência e seus limites
Recuperado em:
https://dialnet.unirioja.es/descarga/articulo/2270935.pdf

7. A ESPIONAGEM COMO INSTRUMENTO DA POLÍTICA EXTERNA DOS ESTADOS UNIDOS DA AMÉRICA E AS CONSEQUÊNCIAS NAS SUAS RELAÇÕES EXTERIORES

8. USB espião profissional - VÁRIOS MODELOS

9. Detector não linear clássico - The Detective and Spy Shop