。  
 敵を誘惑するために餌を差し出します。  
– Sun TzuForceとFraudは、2つの枢機卿の徳を戦っています。  
1はじめに何十年もの間、電子戦争はいくつかの一般的な技術を使用していたにもかかわらず、コンピュータセキュリティとは別の主題でした。  
 2007年のロシアのサービス拒否攻撃はエストニアを攻撃し、多くの政策アジェンダにそれを確固たるものにしています。 Stuxnetはそれをプライムタイムに移行しました。そして、2016年の2つの大きな政治イベントである英国の離脱国民投票と米国の選挙におけるロシアの干渉は、立法者に彼らの仕事にコストがかかる可能性があることを教えた。  
 もともと戦士のために開発された多くの技術は、商業的使用に適合されており、有益な類似点がたくさんあります。  
 主題は1989年の冷戦の終結後に落ち着きましたが、ロシアがその軍隊を近代化し、AIがレーダー、ソナーおよび関連システムへの道を見つけるにつれて、チャイナワークスが米国との競争相手になるために最近復活しました。  
70423。  
 BASICSE電子戦争はまた、サービス拒否攻撃、コンピュータセキュリティの人々が何年もの間無視してきたアトピー、そして直接的および心理的要因の両方を含むハイブリッド攻撃についての最初の教師でもありました。  
23。  
 優先事項は：1。  
 自動化されたシステムまたは人を標的とする可能性のある詐欺。および3。  
教義のレベルでは、電磁戦は一般に次のように構成されていると見なされます•敵の通信やレーダーの妨害などの電子攻撃、および高出力マイクロ波を使用した敵の機器の妨害;•電子保護、これはレーダーおよび通信機能を保持することに関する攻撃の顔。  
 これにより、指揮官は、意図的および非意図的な電磁エネルギーの発生源を検索、特定、および特定できます。  
 暗号化の伝統的なトピック、つまり通信セキュリティ（Comsec）は、現代の民間システムにおける情報保護のほんの一部であるのと同様に、電子的保護のほんの一部です。  
 前者はメッセージの内容と通信しているユニットに関するトラフィックデータの両方を含む敵の通信を収集しますが、後者は敵のレーダーや他の非通信電磁エネルギー源の認識に関係しています。  
 目標は、敵の知性と標的の獲得の精度を低下させるために、敵を彼らの知覚を操作することによって誤解させることです。  
3。  
 詐欺は非常に費用効果が高く、商業システムにますます関連しています。  
 電子戦が成功するかどうかは、利用可能なツールを協調して使用することにかかっています。  
 最初に通信システムの問題について説明します。それらは最も自己完結型であるため、次にセンサーと関連する妨害装置、そして最後に電磁パルス発生器などの他のデバイスについて説明します。  
23。  
 今日、典型的なコマンドと制御構造は、ポイントツーポイントリンクとブロードキャストで動作するデータ、音声、画像をサポートするさまざまな戦術的および戦略的無線ネットワークで構成されています。  
 状況認識と力を指示する手段がなければ、指揮官は効果的でない可能性があります。  
•明白なタイプのトラフィックの1つは、軍の本部などの固定サイトと政治指導者との間の通信です。  
 虚偽のメッセージの挿入は、状況によっては脅威となる場合もあります。  
 二次的な脅威は、ケーブルやリレーステーションの破壊、またはリソースが共有されているトラフィックフローによってリンクが中断される可能性があることです。  
 ここでは、暗号セキュリティに加えて、位置セキュリティも重要です。  
 彼らがインターネットやSecurity Engineering706Ross Anderson23などの敵が監視できる媒体を使用してメッセージを送信する場合。  
 通信システムラジオ、それから一部のエフォートは、イライラするトラフィック分析とラジオダイヤリング発見に入るかもしれません。  
 無線の方向探知は依然として問題ですが、妨害は少なくとも同じくらい重要である可能性があり、故意に欺瞞的なメッセージも問題である可能性があります。  
 音声学習モーフィング技術は、機械学習のディープフェイク技術を使用して開発されているため、通信に対するスプーフィング攻撃のリスクが高まります。  
•航空機から発射したばかりのミサイルに送信される信号などの制御およびテレメトリ通信は、妨害や改ざんから保護する必要があります。一般的な解決策は、通信を適応型にすることです。つまり、妨害の可能性が低いモードで開始し、妨害に応じて必要に応じて電力を増加させます。  
 これらはいくつかの微妙な方法で相互作用します。  
 その考えは、ロシア人が妨害装置をオフにする準備ができていなければ、方向を見つけるのにもっと努力しなければならないということでした。  
ソビエトの教義によれば、軍事通信インフラストラクチャに対する包括的で成功した攻撃には、物理​​的に3分の1を破壊し、妨害、トロイの木馬、または詐欺などの手法を通じて2/3の効果的な使用を拒否し、その後、攻撃者が無効化できるようにします残りの3分の1は、停止している容量の3分の1を超えてすべてのトラフィックを通過させようとします[1156]。  
NATOは、80年代に、カウンターコマンド、コントロール、コミュニケーションのオペレーション（C-C3、発音はC Cの3乗）と呼ばれる同等の教義を開発しました。  
 もちろん、軍の司令部を攻撃することははるかに古いです。部下を撃つ前に、anocerで撃つことは基本的な常識です。  
3。  
3。  
信号インテリジェンスにおける最も高価で重要なタスクは、無線信号の不協和音と電話ネットワークやインターネットなどのシステム上の膨大な量のトラフィックから興味深い資料を特定して抽出することです。  
 多くの場合、信号分析によって個々の機器を識別することができます。  
 このRF指紋（RFID）テクノロジーは、1990年代半ばに複製された携帯電話の識別に使用するために機密解除されました[776、1662]。  
Radio Direction Finding（RDF）も重要です。  
したがって、スパイは、移動する前に家にメッセージを送信するのに数分かかる場合があります。  
トラフィック分析（発信元と宛先ごとのメッセージ数を見る）も非常に貴重な情報を提供します。  
 ただし、トラフィック分析は、公共ネットワークでトラフィックをふるいにかけるときに実際に活用され、その重要性（国家情報および警察の目的の両方）を誇張するのは困難です。  
しかし、今世紀には、トラカナリシスが影から出てきて、主要な研究対象となっています。これについては、法執行機関および第26条の諜報監視のコンテキストで説明します。  
2。  
 アリスのスパイ活動（または麻薬取引など）が疑われる場合は、彼女が電話するすべての人と、彼女を電話するev-eryoneに注意します。  
 あなたは分析するのに多すぎる人々から電話を受けた銀行や医者のようなものを排除し、残りの各番号に対して手順を繰り返します。  
 これで、収集した雪玉をふるいにかけました。たとえば、すでにブラックリストに登録されている人や、複数回表示される電話番号などです。  
 次に、アリスのネットワークを最初に近似する友情ツリーを描画し、それを他のインテリジェンスソースと照合して洗練させます。  
3。  
 主要なアルゴリズムの1つはMark Newman [1434]によるものです。これは、スペクトル法を使用してネットワークを自然なコミュニティに分割し、モジュール性を最大化します。  
しかし、抽象的なネットワークを分析するための優れた数学ツールが与えられても、現実は厄介です。  
共謀者が積極的な対策を講じるとき、それはさらに難しくなります。ボブはアリスから自分の勤務先電話番号に電話をかけ、それから電話ボックスからイブに電話をかけるかもしれません。  
 また、電話番号のトポロジーを関連付けるいくつかの手段が必要になります。  
 IPアドレスを人々に結び付けるのはさらに難しい。 ISPは常にRADIUSログを長期間保持するわけではありません。  
2。  
2。  
 とりあえず、匿名のコミュニケーションは新しいものではありません。  
しかし、匿名のコミュニケーションを適切に使用するために必要な規律はほとんどの犯罪者であるので、それらは詐欺師のための普遍的な答えではありません。  
信号の収集は、電話会社に電話の内容と項目別の請求レコードへのアクセスを許可することだけに制限されていません。  
2。  
 それ以前にも、長い一連のリークと調査ジャーナリストによる作業のおかげで、全体像を把握していました。  
 エシェロンとして知られている、これは、電話、ファックス、データトラフィックを監視する多数の固定収集ステーションで構成され、興味深い電話番号、ネットワークアドレス、機械可読コンテンツについて通過トラフィックを検索する辞書と呼ばれるコンピューターを使用しました。このトラフィックの選択はインテリジェンスアナリストが入力した検索文字列によって駆動されます。世界中に100以上のノードを持つ大規模な分散型検索エンジンになっています。  
 Tra�cデータも保持されますが、それより長くなります。  
たとえば、ヘイガー氏は、1980年代の軍事クーデター中にフィジーで国内通信を監視するためにオーストラリアとニュージーランドの海軍フリゲート艦を派遣したことについて説明した。  
3。  
 たとえば、セクション2で。  
1。  
Snowdenの啓示以来、IPトラフィックの半分以上が暗号化されており、インテリジェンスと法執行の焦点がエンドポイントからコレクションにいくらか移行しています。  
23。  
2通信の攻撃敵のネットワークをマッピングしたら、攻撃したくなるかもしれません。  
まず、一部のシステムは純粋な暗号解読によって破壊されていますが、これはかなりまれです。  
 例には、第二次世界大戦中のアメリカ大使toRomeの係員による国務省のコードブックの盗難[1001]が含まれます。ソビエトの外交軌道に対する「ベノナ」攻撃につながるワンタイムパッドの製造と流通のエラー[1001];また、CIAとドイツのBun-desnachrichtendienstによるスイス企業Crypto AGのカバータウンシップについては、セクション26で説明します。  
7。  
 Ed Snowdenは、GCHQによるGemplusからのカードパーソナライゼーションファイルの盗難を明らかにしました。これにより、何百万ものSIMカードのキーが約束され、インテリジェンスコミュニティは何百万もの携帯電話にアクセスできるようになりました。  
 これは、輸出規制の場合と同様に明白です（セクション4を参照）。  
1と26。  
9）または微妙な、乱数発生器の標準と同様（セクション2を参照）  
1。  
2。  
7）。  
他の州でも同様のゲームを行っています。冷戦時代のソビエトの諜報活動の歴史は、ウォーミン家などの主要な資料を販売した裏切り者を採用するというソビエトのスキル「ヒューミントインシギントのサポートの使用」によって、アメリカの技術的優位性がほとんど失われたことを示しています[118] 。  
2。  
第二に、コンテンツへのアクセスは、しばしば望ましい結果ではありません。  
妨害には、ノイズの挿入だけでなく、能動的な欺瞞も含まれます。  
 前の章で、諜報部隊と作戦部隊の間の緊張について述べました。前者は相手側の信号を聞きたがり、後者はそれらの使用を拒否したいです[150]。  
 それはあなたが読むことができるものを敵に伝えるので、あなたが読むことができないトラヒックを詰まらせるだけでは十分ではありません！セキュリティエンジニアリング710ロス・アンダーソン23。  
 コミュニケーションシステムSMattersは、対戦相手が暗号を使用している場合、特にそれらが有能であり、そのトラフィックを読み取ることができない場合に簡略化できます。  
 これには、ケーブルを掘ったり電話交換を爆撃するハードキルアプローチ（どちらも連合軍が湾岸戦争1中に行ったもの）、妨害のソフトキルアプローチ、または効果的な組み合わせが含まれます。  
 物理的な攻撃よりも効果的であるケースには、衛星リンクが含まれます。アップリンクは、適度な量の電力のみを使用して、隠れた場所からの狭いビームを使用して妨害されることがよくあります。  
 （セルビアの情報戦争セルのボスニア戦争中に、DDoS NATO Webサイトを狙った逸話がありました。  
23。  
3保護技術したがって、通信セキュリティ技術には、真正性と機密性を保護するだけでなく、トラフィック分析、方向探知、妨害、物理的破壊の防止も含まれます。  
 ただし、同期と妨害のトレードオフのため、リンク層の暗号化は無線ではトリッキーです。そして、それだけでは必ずしも十分ではありません。単一のノードを敵が捕獲すると、ネットワーク全体が危険にさらされる可能性があるからです。  
そのためには、異なるテクノロジーが必要です。  
これらの最初の2つのオプションはかなり単純明快であり、実行可能な場合は通常は最適です。  
 大規模な砲撃があったとしても、スターリングラードの電話網は包囲中ずっと（両側で）使用されていました。  
セキュリティエンジニアリング711ロスアンダーソン23。  
 COMMUNICATIONS SYSTEMSA LPI / LPPF /アンチジャムテクニックの数は、スペクトラム拡散通信の総称です。  
 第二次世界大戦前後の初めから、スペクトラム拡散はかなりの産業を生み出し、テクノロジー（特にDSSS）は、Bluetoothなどの無線プロトコルを介して（GPSシステムでの）高解像度レンジから、他の多くの問題に適用されてきました。23。  
3。  
 それらは、その名前が示すとおり正確に動作します。ある周波数から別の周波数に高速でホップし、周波数のシーケンスは、承認されたプリンシパルに知られている疑似ランダムシーケンスによって決定されます。  
 周波数ホッピングレーダーは、ドイツ人によってほぼ同時に独立して開発されました[1682]。  
 ホッピングが遅く、近くの対戦相手が対応可能な機器を持っている場合、オプションはフォロワー妨害、つまり信号を観察し、バンドの周りを追跡することです。通常、連続する各周波数をシングルトーンで妨害します。  
 入力信号の帯域幅と送信信号の帯域幅の比率は、システムのプロセスゲインと呼ばれます。したがって、10 MHzに広がる100ビット/秒の信号のプロセスゲインは107/102 = 105 = 50dBです。  
 ホップシーケンスを効果的に予測できない対戦相手にとっての最適な妨害戦略は、部分的な帯域妨害です。これは、信号に許容できないエラーレートを導入するのに十分な帯域を妨害することです。  
軍事面では、ホッパーは大きな妨害マージンを提供できますが、方向探知に対する保護はほとんどありません。  
周波数ホッパーは実装が簡単で、有効なレベルの妨害耐性を備えているため、man-packradiosなどの戦闘ネットワークで、ホップレートが50〜500 /秒でよく使用されます。  
 高速ホッパー（ホップレートがビットレートを超えるものとして理論的に定義されています。実際には、ホップレートが1秒あたり10,000以上である）は、大きな妨害装置の限界を超えることもあります。  
3。  
1：– DSSSでの拡散（RocheおよびDugelayの厚意による）広帯域疑似ノイズ信号の拡散復調信号復元信号XOR図23。  
23。  
3。  
1と23。  
 これにより、帯域幅が増加してスペクトルが広がります。  
 怒りの最初の展開はベルリン1959年でした。  
 ただし、信号の傍受を大幅に困難にすることもできます。  
 もちろん、ジャム対策信号は高出力で、LPI / LPPF信号は低出力であるため、両方を同時に実行することは困難です。通常の戦術は、敵によって検出されるまで（たとえば、レーダー範囲内に入ったとき）LPIモードで動作し、送信機の電力をアンチジャムモードにブーストすることです。  
3。  
DSSSは「RFの暗号化」と呼ばれることもあり、さまざまなバリエーションがあります。  
 基礎となる数学と技術の古典的な紹介は[1525]です。エンジニアリングの複雑さは、さまざまな理由で周波数ホップよりも高くなります。  
 1つの戦略は、ユーザーに基準信号を提供することで交代させることです。  
 2000年に、フランスが競争相手であった契約であるギリシャ政府に250台の戦車を売ろうとするイギリスの入札を妨害しようとしてフランスがGPS inGreeceを妨害したことが報告されました。  
 策略が発見されたとき、ギリシャ人はかなり面白かった[1918]。  
23。  
3。  
 タイムホップとも呼ばれます。  
 彼らはしばしば特殊部隊と諜報員のためにラジオで使用されます。  
興味深い変種は、流星バースト送信（流星散乱とも呼ばれる）です。  
 母局は継続的に送信します。娘の1人がそのような領域内にいるときはいつでも、母親の声を聞き、高速でデータのパケットを送信し始め、母親はそれに返信します。  
 流星バースト通信は、特殊部隊、および第三世界の遠隔地での降雨の監視などの民間用途で使用されます。  
 低ビットレートと高レイテンシは許容できるが、機器のサイズとコストが重要なニッチ市場では、流星散乱は打ち負かすことが難しい場合があります。  
セキュリティエンジニアリング714ロスアンダーソン23。  
 コミュニケーションシステム23。  
3。  
 また、掃引周波数妨害（妨害波がターゲット周波数帯域を繰り返し掃引する）やフォロワーなどの特殊な妨害技術に直面しても、動作は異なります。  
エンジニアリングトレードもある。  
 一方、DSSS信号は、方向探知技術を使用して位置を特定するのがはるかに困難です[673]。  
 1つのラジオをキャプチャして現在の主要な資料を抽出した相手がこれを使用してネットワーク全体を妨害することを防ぐことは、おそらく重要です。  
•DSSSとホッピングの両方がNATOで知られているように、リンク16のTDMAで使用されます。米軍には戦術デジタル情報リンク（TADIL）としても知られており、以前は合同戦術情報配信システム（JTIDS）[1662]として知られていました。57のDSSS信号があります。  
5dB）、これは255MHz帯域でホップして、最低30MHzのジャンプをします。  
 理論的根拠は、機器のキャプチャが拡散コードの侵害につながる場合、255 MHz全体ではなく、単一の10 MHz帯域のみの妨害を可能にするということです。  
•米軍は、静止軌道からの1度のビームを備えた一連の衛星通信システム（MILSTARおよびDSCS）によってサポートされています。  
 ジャム防御はホッピングによるものです。そのチャネルは、2 GHzの帯域で1秒あたり数千回ホッピングします。  
 兵士は無線機から100ヤードの距離でハンドセットを使用できます。  
セキュリティエンジニアリング715ロスアンダーソン23。  
 通信システム干渉除去などのシステムレベルのトリックもあります。これは、自分の無線で認識されている波形と妨害している帯域で通信するため、それらをキャンセルしたり、周囲を飛び回ったりすることができます。  
23。  
4市民と軍事利用の相互作用市民と軍事のコミュニケーションはますます絡み合っています。  
相互依存性が高まっているもう1つの例は、全地球測位システム、GPSです。  
 湾岸戦争1の間にこれをオフにする必要がありました。周回するのに十分な軍用GPSセットがなく、代わりに民間機器を使用する必要があったからです。  
 最後に、2000年5月、クリントン大統領は、選択的可用性の終了を発表しました。  
 しかし、今では非常に多くの多様なシステムが、GoogleマップからUberまでGPSに依存しているため、責任ある政府がそうすることはほとんどありません。  
 セクション14で説明したように、一部の国では、GPSを使用して道路の価格設定をしたり、電子足首タグを介して解放された囚人に仮釈放条件を適用したりしています。  
 安価なデバイスの範囲は短く、通常は5〜10mです。  
 例としては、位置Aで信号をサンプリングし、位置Bで信号を再送信するミコニングがあります（これは、ワームホール攻撃とも呼ばれます）。  
 これは一部の政府首脳のリムジンで防御メカニズムとして使用されます（高度な暗殺者がこれを使用してミサイルを標的にすることができます）。  
 スプーフィングは、既知の場所にある別の受信機を参照ポイントとして使用する差分GPS（FAAのトリック）を使用して、およびS-GPSとも呼ばれる干渉GPSを使用して、ほとんどが検出できます。合成開口を生成するための受信機。  
4。  
米国のGPSシステムに加えて、ロシア、中国、ヨーロッパには、同じ原理を使用する個別のナビゲーション衛星システムがあります。総称して、このようなシステムはGNSSとして知られています。  
4監視と標的獲得標的獲得と武器ガイダンスに関連する電子戦のこれらの側面は、妨害と欺瞞の芸術が最も高度に開発されてきた場所です。  
）敵対的なターゲットを検出し、武器をそれらに誘導するために使用される主な方法は、ソナー、レーダー、赤外線です。  
その他の主要なセンサーはレーダーです。  
そのために開発された電子攻撃および保護技術は、他のセンサーを使用するシステムよりもよく開発されており、多くの場合、それを超えています。  
4。  
 それらはさまざまな信号特性を持っています。  
 テクノロジーに関する古典的な教科書は、シュレアー[1662]によるものです。  
 デジタルエレクトロニクスの前の時代には、ディスプレイチューブのスイープをアンテナと同期して機械的に回転させることができました。  
 これで、ビームは複数のアンテナエレメントを使用して電子的に生成されますが、トラッキングループは中心のままです。  
これは、一般的に角度分解能と追跡パフォーマンスに影響を与えます。  
セキュリティエンジニアリング717ロスアンダーソン23。  
 監視とターゲットの取得ドップラーレーダーは、戻り信号の周波数の変化によってターゲットの速度を測定します。  
 ドップラーレーダーには、アンテナに対する半径方向の速度が特定の制限内にあるターゲットへの注意を制限する速度ゲートがある場合があります。  
 これはレーダーを使用して、相対速度が大きすぎる（対向車でパニックにならない）車両や、遠すぎたり遠すぎたりする車両を無視するようにゲートされています。  
23。  
2妨害技術電子攻撃は、受動的または能動的です。  
第二次世界大戦の終わりに向かって、同盟国の航空機はドイツの航空防衛を低下させるために1日あたり2000トンのチャフを落としていた。  
 チャシュに対する主な対抗手段はドップラーです：アッシャシュは非常に軽く、ほとんど一度に休息するようになり、動くターゲットからかなり簡単に区別できます。これらの原則は非常に一般的です。  
最も多くのお金が費やされた受動的対策はステルス–車両のレーダー断面積（RCS）を減らし、非常に短い範囲でのみ検出できるようにします。  
 ステルスには幅広いテクニックが含まれており、適切な議論はこの本の範囲をはるかに超えています。  
 航空機のRCSは通常、その側面の機能であるため、特定された敵のエミッターに低RCSaspectを継続的に示すフライバイワイヤーシステムを備えている可能性があります（F117はパイロットに「ぐらつくゴブリン」として知られるようになりました）。  
 初期の妨害装置は、ターゲットレーダーが使用する周波数範囲で大量のノイズを発生させていました。これは、ノイズ妨害または弾幕妨害として知られています。  
 しかし、そのようなセキュリティエンジニアリング718ロスアンダーソン23。  
 監視と目標の取得信号をブロックするのはかなり簡単です。1つのトリックは、ガードバンドレシーバー、使用中の周波数に隣接する周波数のレシーバーを使用し、このレシーバーが妨害信号を拾ったときに信号をブランキングすることです。  
もう一方の端にあるのは、敵対的な信号に乗っている支援航空機によってしばしば発射される対放射線ミサイル（ARM）などのハードキルテクニックです。  
真ん中には、詐欺妨害技術の大きなツールキットがあります。  
自己防衛妨害装置の通常の目標は、攻撃者に範囲と方位情報を拒否することです。  
 これは、攻撃者のアンテナの指向性が通常完全ではないという観察に基づいています。ビームはメインローブと同様にサイドローブを持ち、それを介してエネルギーも送受信されますが、効率ははるかに低くなります。  
 攻撃者のレーダーに関する限り、信号はどこからでも発信されているように見えます。レーダー画面の「ブリップ」の代わりに、自分のアンテナを中心とした円が表示されます。  
より一般的には、この手法は、遅延および/または周波数の系統的変化を伴ってレーダー信号を再送信することです。  
 最新の機器は、受信した波形をデジタル無線周波数メモリ（DRFM）に保存し、信号処理を使用して操作します。  
 パルス繰り返し周波数を下げると、滞留時間が長くなり、戻り信号が強くなりますが、精度は低下します。  
 ここで、妨害装置は、実際のパルスよりも強力な多数の偽パルスを送信して、レシーバーを捕捉し、ターゲットをレシーバーのレンジゲートから外すように位相をずらします。  
 古いレーダーでは、RGPOが成功すると、レーダーがロックを解除し、ターゲットが画面から消えます。  
基本的な対策は、パルス繰り返し周波数にジッタを与えることです。  
4。  
このような追従妨害は、遠くにあるように見える誤ったターゲットのみを作成できます。  
 別の方法は、妨害パルスが最大ジッタ周期をカバーするのに十分な長さである妨害妨害です。  
 Cha↵は、アラダーをドップラーモードに強制するためによく使用されます。これにより、PRFジッターが困難になります（連続波形は、ドップラーのパルスよりも優れているため）。  
 もちろん、デザイナーが賢すぎることは常に可能です。 Mig-29は、一部のレーダー設計者が予想していたよりも、急激な引き上げによってレベルフライトでより速く減速する可能性があるため、パイロットはこの操作を使用してレーダーロックを解除できます。  
23。  
3高度なレーダーと対策妨害から守るために、いくつかの高度な技術が使用されています。  
 これにより、10〜1000の処理ゲインが得られます。  
 ただし、LPI波形を使用することは、ターゲットを検出するずっと前にターゲットに検出させたくない場合に重要です。  
 これは多くのハイエンド市場を支配するようになり、たとえば、飛来者の侵入に対する防空のためのルックダウン射撃システムで広く使用されています。  
 多くの脅威に対処しなければならない航空機搭載レーダーは、高いPRFを使用し、100ノットなど、あるしきい値を超える速度のみを探しますが、テールチェイスには弱いです。  
 また、検索レーダーには長く多様なバーストが必要ですが、追跡には短く調整されたバーストのみが必要です。  
 パルスドップラーに対して使用される主な詐欺戦略は、速度ゲートのプルオフですが、現代のバリアントは、偽のリターンで複数の速度ゲートを励起することです。これは、例えば、フォークランドセキュリティエンジニアリング720ロスアンダーソン23で妨害するのが非常に困難であることが証明されたExocetミサイルで使用されました。  
 監視と目標の取得戦争。  
モノパルスレーダーは、設計上の欠陥が悪用される可能性がない限り、妨害するのが困難で費用がかかります。通常のテクニックには、フォーメーションジャミングや地形バウンスなどのトリックが含まれます。  
強力なトリックの1つは、パッシブコヒーレントロケーションです。  
受信者は受動的であるため、場所を特定して攻撃することは困難です。システムをノックアウトすることは、主要な民間のインフラストラクチャーを破壊することを伴います。反対者は、法的および宣伝上の理由でそうしないことをしばしば好むでしょう。  
 パッシブロケーションは実際にはレーダーの先駆者である1930年代のロバートワトソンワットに遡り、クラインハイデルベルクのステーションがイギリスのチェーンホームレーダー信号を利用してRAF航空機を追跡したときに、最初にドイツ人によって使用されたようです（EWの用語では、ヒッチハイカーでした） '）。  
2020年の1つの研究フロンティアは、認知レーダーです。  
 レーダーと妨害波の両方の波形は、以前よりはるかに高い柔軟性で戦術的な状況に適応できます。  
 その瞬間からレーダー（またはソナー）がオンになり、その環境に関する知識が蓄積されます。その興味深い側面はほとんどが動的です。  
 これは非協力的な目標と対立するものになります。  
23。  
4その他のセンサーとマルチセンサーの問題私がレーダーについて述べたことの多くはソナーにも当てはまり、かなりの量の赤外線が当てはまります。  
 フレアはチャ↵に似ており、ターゲットに対して急速に減速するため、攻撃者は速度や加速をフィルタリングできます。  
アクティブな赤外線妨害は、レーダー妨害よりも広域性が低いため、あまり普及していません。それは混乱を引き起こすレートまたはパターンで脈動することによって敵対的なセンサーの機能を悪用する傾向があります。  
5。  
成長分野の1つは、マルチセンサーデータの融合です。これにより、レーダー、赤外線センサー、ビデオカメラ、さらには人間からの入力が組み合わされて、個々のターゲットよりも優れたターゲットの識別と追跡が可能になります。  
 データの融合は、見かけよりも難しい場合があります。  
図８に示すように、２つの警報システムを組み合わせると、一般的に、誤警報または見逃した警報率のいずれかが改善され、他方が悪化する。  
攻撃者が船や航空機などの反撃に対して脆弱なプラットフォーム上にいる場合、状況はより複雑になります。  
 通常のトリックは、ランダムな時間に短い「ルックスルー」期間にわたってジャメロをオンにすることです。  
冷戦中は、両側に高出力の専用装置を備えた専門家の支援車両が必要であり、ある程度のエネルギー闘争になります。これは「ワット数が最大の勝利」です。  
 （ステルス時の）妨害の全体的な影響は、レーダーの有効範囲を狭めることです。  
23。  
 フレンドまたは敵を特定するシステム（IFF）は、重大かつ論争の的であり、米国と連合軍との間の機器の非互換性が原因で、イラクで発生した「ブルーオンブルー」の事件が多数発生しています。  
IFFは非技術的な形で古代に戻ります。  
 WorldWar 2は、フランスの抵抗が人々に「グルヌーユ」を発音するように求めるのを見ました、そして、できなかった人はドイツ人であると推定されました。  
5。  
 ドイツの飛行機は、レーダーの断面に「ブリップ」を作成するために、ラジオオペレーターが挑戦したときにロールオーバーしました。  
朝鮮戦争により、ジェット機とミサイルの両サイドに到着したため、視覚的にターゲットを特定することは現実的ではありませんでした。  
レガシーNATOシステムは、1960年代に導入され、セクション4で説明したプロトコルの問題を解決するために設計されたMark XIIです。  
3。  
 チャレンジまたは応答が長すぎると、レーダーのパルス繰り返し周波数（およびその精度）が低下します。  
 効果は、敵がnullまたはランダムな応答を持っている間、「友達」は中央画面の近くにクラスター化された応答を持ち、それが点灯するということでした。  
 （チャレンジに使用されるアンテナは通常、古いシステムでは円錐形にスキャンされた火の制御レーダーです。  
 このようなシステムには、民間航空機がIDを2次監視レーダーに「揺さぶる」ために使用するシステムとの互換モードもあります。  
 NATOのIFFシステムは、アイアンカーテンの両側にある何千もの戦術航空機の冷戦シナリオのために進化しました。イラクやアフガニスタンのような現代の紛争では、どのように対処しますか？歴史的に、犠牲者の約10〜15％は「友好的な火」によるものでしたが、湾岸戦争1ではこれが25％に増加しました。全国的なシステムが異なるため、連立作戦もリスクを増大させる。  
 しかし、湾岸戦争が起こったとき、何もきちんと配備されていませんでした。  
 国防だけでなくサービスによっても、これらのサービス内の派閥によって防衛が購入される世界で、そして議員が同盟国との技術的協力を阻止することによって（それらを止めるために）教育を受けていない有権者に彼らの「愛国心」を合図しようとする世界で私たちの仕事と私たちの秘密を盗みます '）、制度的および政治的構造は、NATO全体で機能する適切なIFFシステムなどの防衛「公共財」を提供するのに役立ちません。  
”セキュリティエンジニアリング723ロスアンダーソン23。  
 爆破装置の改善プロジェクトの複雑さは1つの問題です。空軍の飛行機同士の射撃を停止することはそれほど難しくありません。また、船や戦車で射撃を停止することははるかに複雑です。さらに、12か国が関与している場合はさらに困難です。  
 彼らはモバイル戦争の力の能力を大幅に高め、ユニットがお互いのキルゾーンをドライブするような危険な作戦を実行できるようにしますが、2000年代後半から2010年代初頭のイラクのような複雑な戦争の万能薬ではありません。また、信頼性が不明なノードを持つネットワークを自動化することは困難です[1659]。  
 しかし、これはペンタゴンで最大の調達失敗の1つであり、使用可能なラジオを1つも提供せずに15年間で60億ドルを費やした[1983]。  
 NATO内で20年以上争っていたアメリカは、防衛産業が激しく働きかけている高価なハイテクシステムを求めていましたが、ヨーロッパ諸国は、たとえば通常のコマンドでユニットを追跡するなどして、よりシンプルで安価なものを求めていました制御システムと国家間のまともなインターフェイスを持っています。  
アメリカは同盟国の組み合わせよりも防衛に多くを費やし、それが先導すべきだと信じていました。同盟国は、米国のサプライヤへの依存がさらに高まることで、自分たちの能力がさらに取り残されることを望んでいませんでした。  
 ドナルドラムズフェルドが推進し、システムの電子システムに基づいた「革命革命軍（RMA）」は、同盟国の予算を超えているだけでなく、広大な地域を通じて自分の犠牲者を最小限に抑えることに不信を抱いていた物質的および技術的優位性。  
 これに対するアメリカ人のレトルトは、ヨーロッパが弱すぎて、ボスニアでの大量虐殺にさえ対処することができなかったということでした。  
 イラクとアフガニスタンの同盟軍は、車両の屋根に大きなカラーパッチを塗装し、空爆が通過することを望んでいた。  
 脱グローバリゼーションとトランプ大統領の外国の同盟国に対する焦りを考えると、今何が起こるかは誰にも分からない。  
6即席爆発装置電子工学的対策において、セキュリティエンジニアリングでロス武装勢力が選択した武器である即席爆発装置（IED）に対抗するための重要な試みが行われた724ロスアンダーソン23。  
 改良型爆発装置SIraqとアフガニスタン。  
S  
機関銃は第一次世界大戦であり、レーザー誘導爆弾は第一次湾岸戦争であったため、これらの爆弾はイラク戦争の「特徴的な武器」となった。  
とにかく、33,000以上の妨害装置が作られ、連合軍に出荷されました。  
 効果として、ラジコンIEDの比率が70％から10％に低下し、コマンドワイヤーによってトリガーされる比率が40％に増加しました。  
 他の多くの民族主義者および反乱グループは、第二次世界大戦でのロシアの抵抗、Irgun、ETA、およびベトコンからアイルランドの民族主義者まで、アナキストからIEDを使用してきました。  
 彼らはまた、20世紀の多くの機会にイギリスに対して爆撃キャンペーンを行った。  
 IRAとの対戦には合計で約7,000のIEDが関与し、英国の防衛科学者に妨害の経験を豊富に与えました。  
イラクの電子環境は、ベルファストやパキスタンのどちらよりもはるかに困難であることが判明しました。  
 一方、イラクのRF環境は複雑で混沌としたものになりました。  
 150,000の連合軍も多種多様なra-dio排出量を送りましたが、部隊が交代すると常に変化しました。連合軍は、何百人もの海軍の電子戦の専門家がバグダッドに配備されたときにのみ問題に取り掛かり始めた。その後、連合の妨害妨害はより適切に調整され、無線で爆発したIEDの割合を削減し始めました。  
IEDメーカーは、単にラジコン爆弾から、プレッシャープレート、コマンドワイヤー、パッシブ赤外線、またはボランティアによって爆発させるデバイスに切り替えました。  
7。  
 2003年にはほぼすべてのIEDが連合軍の死傷者を引き起こしたが、2007年までに平均で4つのデバイスが使用された[140]。  
ただし、ネットワークの混乱は、人間の知性の優れた情報源の構築に依存しているため、長期的な影響があります。英国とイスラエルは、それぞれアイルランドとレバノンの爆弾製造業者を標的にして何年も過ごしました。  
7Directed Energy Weapons1930年代後半、イギリスとアメリカでは、ナチスが車両発火システムを焼き尽くす高出力無線ビームを開発したという噂がパニックになりました。  
 それらは正しかった–比較的低出力の無線送信機と、1930年代のシンプルだが堅牢な車両用電子機器を考えると。  
 核デバイスのデトネーションは、ガンマ線光子の大きなパルスを生成し、次に、コンプトン散乱によって空気分子から電子を移動させます。  
核爆発が地球の大気内で発生する場合、EMPenergyは主にVHF帯域とUHF帯域にありますが、無線フラッシュが数千マイル離れた場所で観測されるのに十分なエネルギーが低い周波数にあります。  
 地球の大気圏外での爆風の影響は、はるかに悪いと考えられています（テストはこれまでありませんでしたが）。  
 北ヨーロッパのほとんどの電子機器は、北海から250マイルの高さで1メガトンの爆風によって燃え尽きる可能性があると推測されています。  
そのような攻撃は誰も直接殺さないでしょうが、コロナウイルスの大流行の規模で経済的損害を引き起こすかもしれません[122]。  
電信システムはヨーロッパと北米の至る所で故障し、時々彼らのオペレーターに電気ショックを与えました。  
 小さい地磁気嵐が定期的に、たとえば1989年と2003年に起こります。  
8。  
EMPに関する西側の懸念は、ソビエト連邦が80年代半ばに非核EMP兵器に関する研究プログラムを開始した後に高まりました。  
 ソビエトはこれを、財産をそのままにしながら人々を破壊する「資本主義爆弾」として描写し、「社会主義爆弾」を脅迫して周囲の人々を傷つけずに（電子機器の形で）財産を破壊すると対応した。  
 バルブからトランジスタおよび集積回路への移行により、ほとんどの商用電子機器の脆弱性が増大しています。  
 実際、銀行の地下サーバーファームは影響を受けない可能性があります。本当のダメージは日常の電子機器にあります。  
戦場で使用する場合、EMP兵器はトラックにマウントする必要はなく、標準爆弾または砲弾ケーシングに収めることが望ましいです。  
 米国は、IEDで電子機器を揚げる手段としてイラクでBlow Torchと呼ばれるデバイスを試しましたが、うまく機能しませんでした[140]。  
 しかし、航空機から投下されたEMP爆弾は、適切な結合を得るために、爆発の前にアンテナを配備する必要があり、半径が数百メートルしかないため、通常の電子機器にとって致命的でさえあります。  
EMPの真の意味は、原始的な核技術を用いてイランや北朝鮮などの国々に脅迫兵器を与えることかもしれません。  
」日本は現在、ミサイル防衛を開発しています。  
この観察はインターネットへの攻撃にも当てはまるので、次に「情報戦争」に戻りましょう。  
8情報戦争情報戦争というフレーズは、1995年頃から使用されています。  
 そこでは、陸上攻撃が開始される前に空軍力がイラクの防御力を低下させるために使用され、同盟国を支援するNSA要員の1つの目標は最初の攻撃を可能にすることでした。セキュリティエンジニアリング727ロスアンダーソン23。  
 情報警戒要員は犠牲者なしで作られるべきである–たとえイラクの防空壕がその当時無傷で注意深くあったとしても。  
 （1990年までに、USArmyはすでにウイルス生産の入札を求めていました[1206]。  
 軍事計画立案者やシンクタンクは、成功をどのように構築するかを検討し始めました。そこで、政府は古いソビエトの暖かい銃を移動することによってロシアを怒らせました、そしてその後すぐに、国はロシアから発信されたように見える多くの分散したサービス拒否攻撃を受けました[525]。  
ロシアは否定的でした。パケットストームはロシアのボットネット遊牧民によって開始され、エストニアからのニュースに反応し、チャットルームを介してお互いに攻撃しました。攻撃で有罪判決を受けた一人の男性は、エストニア自体の民族のロシアのティーンエイジャーでした。  
エストニアはまた、彫像の撤去に異議を唱える騒々しい民族のロシア人によって引き起こされたいくつかのマイナーな通りの妨害をしました。  
2。  
国家は自衛または他の何らかの正当な正当化と武力紛争の法則に従って行動しなければならない。  
 しかし、通訳は弁護士を忙しくさせてしまうかもしれません。  
セクション2。  
3、私はエストニアが後のウクライナでのロシアの活動のためのウォームアップであったことを説明しました。ロシアは電力インフラを破壊し、NotPetyaワームによってそこで事業を行っている企業に重大な損害を与えました。これは、いくつかの国際企業に重大な付随的損害を与えました。その国。  
。  
 従来の攻撃や操作の前に敵を盲目にするための前駆体兵器として（情報兵器）を使用する必要があります。  
8。  
しかし、当時最も先見の明のあるアナリストは海軍大学院のドロシー・デニングで、そのトピックに関する1999年の本は情報戦争を「敵対するいくつかのアドバンテージを獲得するために情報メディアを標的とする、または悪用する作戦」と定義していました[539]。  
後の記事で、彼女はプロパガンダにおけるネットの役割とコソボ戦争を取り巻く活動について論じた[540]。  
 彼は、情報の優位性を「情報の途切れのない流れを収集、処理、および流布しながら、同じことを行う敵の能力を利用または拒否する能力」と定義しました。  
 この本は、デニングほどコンピュータセキュリティの問題に関する技術的な詳細はありませんが、情報操作の軍事的法理を定式化する最初の試みを示しています。  
8。  
 グリッドを下るのは、核攻撃のサイバー相当物です。電力供給が停止すると、現代の経済における他のすべての機能が停止します。  
 そしておそらく、最近の史上最悪のテロリスト「ニアミス」は、ロンドンに電力を供給する大きな変電所で変圧器を爆破する1996年のIRAの試みでした[231]。  
 最後に、送電と配電への攻撃は、セルビアからイラクへの戦争における標準的な米国の戦術でした。  
）電力網や石油化学プラントなどの資産を管理するために使用されるプロトコル、つまりModbusやDNP3は、プライベートネットの世界で進化したため、セキュリティを研究する人たちは2000年代中頃に制御システムに注意を向け始めました。 -works –インストール内の固定LANとそれらをコントロールセンターにリンクする専用線  
 いたずらによる事故が1〜2回発生した後、セキュリティエンジニアリング729ロスアンダーソン23。  
 情報の警戒と2000年にオーストラリアのマルーチーで水道会社のIT請負業者の不満を持った従業員が下水800トンの流出を引き起こした事件[7]により、制御システムのセキュリティ研究コミュニティが出現し始めました。  
 米国エネルギー省と国土安全保障省は2006年にイニシアチブを立ち上げ、大規模電力システムの基準を設定するNorth Ameri-Can Electric Reliability Corporation（NERC）は、重要なインフラストラクチャ保護（CIP）規格で定められており、ブラックスタート機能には、基本的な情報セキュリティコンプライアンスが必要です。  
 業界の対応は、規制されたコストベースに情報セキュリティを追加できなかったために、一部の石炭火力発電所がディーゼルプラントを廃棄したため、最終的に収益が下がったというものでした[104]。  
 変電所には3つの主要ベンダーがあり、1つがプロジェクトの主契約者になると、通常、他の2つからコンポーネントを購入するため、互換性が不可欠です。  
 脅威モデルも興味深いものです。  
 したがって、変電所のLAN上のトラフィックを暗号化するか、認証するだけでも意味があり、制御トラフィックの一部には4ミリ秒のレイテンシ要件があるため、これを行うことは困難です[731]。したがって、この研究プログラムの実用的な成果の1つは、エネルギー企業やその他の公益事業がネットワークを再境界設定することでネットワークを保護できるようにすることに重点を置いた新興企業でした。  
2番目の結果は、国の電力供給に対する間接的な脅威への意識の高まりでした。  
2。  
 GCHQは設計に関与しましたが、7年後でさえ、「改善された」仕様に準拠しているのは少数の英国のスマートメーターだけです。  
2。  
3番目の結果は、一連の調査ツールでした。  
 Ariana Mirianと同僚による2016年のスキャンでは、変電所からセキュリティエンジニアリング730ロスアンダーソン23まで、世界中で約60,000の脆弱なデバイスが見つかりました。  
 政府の建物内の情報WARFAREto HVAC;彼らはまた、ハニーポットを使用して、そのようなデバイスをスキャンするアクターを追跡しました。半数以上が既知のセキュリティ会社からのものでしたが、かなりの少数が中国またはシールドされたホストからのものでした[1321]。  
 制御システムのセキュリティ研究の初期にさかのぼる、地下犯罪フォーラムの監視により、犯罪グループによる制御システムのハッキングへの支持されていない有能な関心が検出されたため、そのような活動の大部分は国家活動家またはその代理人によるものであると想定するのが妥当です。 。  
 当時、米国の規制強化に関与し、Scadaのセキュリティ会議のいくつかを主催していたIdaho National National Labsが、NSAとイスラエルのカウンターパートがStuxnetワームの開発を助け、それがイランのウラン濃縮能力を破壊したと報告されています2008〜2010年。これについてはセクション2で説明しました。  
1。  
最後に、セクション2で説明したように。  
2015年3月、ロシアはクリミアの配電に対する従来のウクライナの攻撃（ロシアが併合したウクライナの領土）に30のウクライナの変電所を破壊し、230,000人を数時間暗闇にさらしたサイバー攻撃によって対応した[2067 ]。  
 他の制御システムへの攻撃がありました。特に、イランは2020年4月に農村部の水道に有毒なレベルの塩素を導入する目的でイスラエルの配水システムをハッキングしようとしましたが、イスラエルはこれを検出して阻止しました。  
しかし、主な行動は別の場所に移動しました。  
8。  
 エクスプロイタブルな脆弱性のために地下市場で支払われた価格は急上昇し、明白な市場の脆弱性に加えて、セキュリティ研究者がサイバー武器メーカーへの再販のためのアイデアを取ることができる灰色の市場が開発されました。  
 2007年のエストニアと2008年のジョージアへのロシアの攻撃は、2008年のYouTubeに対するパクイスタンによる攻撃と同様に、ある程度心を集中させました（パキスタンは自宅でのみサービスをブロックする予定でしたが、それによって引き起こされたBGP攻撃は世界的な停電を引き起こしました）。 2010年に発生した、China Telecomがインターネットアドレスの15％を18分間ハイジャックした事件。一部の観測者はこれを「サイバー核」のテストと解釈した。  
8。  
 セクション21で主な調査結果について説明しました。  
BGPセキュリティについては1。  
対戦相手が先進国で数日間インターネットを停止できた場合、結果はカオスになることも事実です（特に、さらに多くの人間の活動がオンラインで強制されているため、コロナウイルスの流行により）。  
 ただし、グレートファイアウォールを使用してインフラストラクチャをインターネットの残りの部分から分離し、地元のチャンピオンに代わってGoogle、Facebook、Twitterなどの米国のサービスプロバイダーを除外するというポリシーのため、中国は主に無力です。  
 ロシアは中国に追随しており、Vkontakteなどのサービスプロバイダーはヨーロッパやアメリカのインフラストラクチャとより密接に絡んでいるため、プーチン大統領は2019年5月に法律を可決し、11月までにロシアのISPが外国のインターネットインフラストラクチャとは独立して動作できるようにすることを要求しました。  
 それが機能するようになった場合、ロシアは中国と同様に、残りの世界でインターネットに対する大規模な破壊攻撃を仕掛ける立場にあります。  
8。  
 この期間は、セクション26で詳しく説明するArabSpringで始まりました。  
1。  
 セクション2で説明しました。  
4どのようにしてアラブ政府は西部とイスラエルから監視技術を飛び出し、元NSAの傭兵を雇って、国内外の敵を追跡し、嫌がらせをしました。ロシアには管理選挙の長い歴史があります。  
 その頭、将軍スタロボイトフはoldKGBタイプであると報告されました。彼の代理店はエリツィン大統領に直接報告し、エリツィン大統領は彼の後継者であるプチナスを選んだ。  
セキュリティエンジニアリング732ロスアンダーソン23。  
 セクション2で述べたように、2012年の選挙までに情報戦  
3、ロシアの人口はプーチンが公的支援を結集するために外部の敵の必要性を感じたと十分に穏やかでした。  
 このキャンペーンには、「リトルグリーンマン」（記章のない制服を着たロシアの兵士、ウクライナの反ファシストであると主張）を組み合わせた「ハイブリッド戦争」の戦術が含まれ、さまざまなサイバー攻撃、宣伝、さらにはウクライナのメディアへの攻撃でさえ、虚偽の報告をしましたその親ロシアの候補者は選挙で勝利した。  
 同時にファシズムのアイデアを公然と推進すること–自宅でのイヴァン・イリンのイデオロギーを含む–プーチンはヨーロッパにも残った反ファシストの帯の同情を維持することに成功しました。  
このような情報戦争で使用される戦術は、電子戦争と多くの共通点があります。  
 住民がニューヨークタイムズを読まないようにできない場合は、信じないようにしてください[474]。  
 多くの政治家は他のデコイを使って、報道を混乱させるニュースからマスコミをそらす。トランプは、WHOからヒドロキシクロロキン[1710]まですべてを使用しました。  
 対放射線ミサイルに相当するものは、対戦相手のウェブサイトをブロックしたり、資金を絞ったりしている可能性があります。  
したがって、選挙の安全性は匿名だが検証可能な投票自体の集計に限定されていると考えるのは誤りです。  
 未熟な民主主義でさえ、政治家はフランチャイズとキャンペーンのファイナンス制限などのキャンペーンのルールを操作しようと永遠に試みています。  
 これらの違反の開示は、投票の再審議につながらなかった。それは単に英国の政治を3年間麻痺させる手助けをしただけです。  
結果は、敵の行動よりも有権者間の不満と自己満足の政治家による誤解によるものでしたが、有害な結果を積極的に促進する敵の存在は助けにはなりませんでした。  
8。  
その年の後半の米国大統領選挙についても同様のコメントができる。セクション26で、政治学者のヨチャイベンクラーによる偽ニュースの選出への影響に関する分析について説明します。  
2。  
2。  
 クリントンが選挙に勝ったならば、ハッキングされた選挙システムの証拠がトランプが敗北を受け入れることを拒否することを可能にするために現れたであろうと私は思います。  
 選挙制度は警報のようなものです。セクション13で説明したように。  
 選挙の本当の顧客は敗北した政党であり、政党の1つが敗北を受け入れる準備ができていない場合は、口実で十分かもしれません。  
中国は他国の内政に干渉することを大いに控えています。セクション2で説明したように。  
2、彼らは長い間、無検閲のインターネットは米国の共産党支配の転覆に相当するという見方をしてきましたが、その前線での彼らの姿勢は防御的でした。  
 セクション2で説明するように、このキャパシティビルディングは、特に米国でHuaweidomination 5Gインフラストラクチャを阻止するという政治的影響をもたらしました。  
2と22。  
4。  
 2020年には、中国がコロナウイルスを巡る物語を定着させ、パンデミックに対する米国の無秩序な対応を利用しようとするため、より積極的な外交の兆候があります。  
8。  
 それには歴史的な先例があります。  
その間の20年の間に、名称は変わりました。国防総省は1998年に「情報戦」を採用し、2006年に「情報作戦」に、2013年に「サイバースペース作戦」に変更しました[1164]。  
その間、多くの間違った考えは徐々に捨てられてきました。  
9。  
 他の人たちは、情報戦争が負傷者のない勝利の方法を提供したと示唆していた。「イランの電力網をハックして、彼らが平和を訴えるのを見てください」。  
 さらに、NATOの国が侵略者である場合、タリンのマニュアルは検察を強化します。  
 これまでのところ、ロシアによる開発が、ジョージアとウクライナで磨かれたハイブリッド戦争戦略のコンポーネントに発展しているのを見てきました。  
 アメリカ、ロシア、中国が国連の下でお互いに首をかしげながら優しく笑顔を続けているので、これは今後10年間の未来でもありますか？それとも他の可能性はありますか？アラブの春の平和的なデモ参加者や中東の暴力的な過激派がサイバー戦術を利用しているところを見てきましたが、ほとんど成功していません。9要約電子戦は冷戦中に発展し、多くの興味深い技術を開発しました。そのうちのいくつかは主流の情報セキュリティへの道を見出しています。  
 AI革命は、ゲームがコグニティブレーダーおよびソナーとして再生される方法を変える可能性があり、マルチセンサーデータフュージョンのためのより優れた技術と相まって、最大メガワットのプラットフォームから、最もスマートなソフトウェアを備えたプレーヤーに利点をもたらします  
10年前、人々はすでに電子戦争が情報戦争になることについて話しました。  
 そして、国家の関係者が他国の重要な国家インフラを攻撃するための準備をしていることは容易に観察できます。  
 おとり、妨害、および敵のレーダーを操作するために使用されるその他の技術と、世論を操作するために使用される技術の間には、いくつかの興味深い類似点があります。  
 まず、私たちは敵対的な機械学習に注目してきました。  
9。  
 私たちは、組み込みシステムを狙った攻撃を含む、攻撃トラフィックをキャプチャするためのより良いハニーポットを開発します。  
 彼らは今、政治的過激主義とサイバー犯罪のために地下のフォーラムのインクルードを始めています。  
 スペクトラム拡散シーケンスのアンチジャムプロパティの古典的な紹介は、Andrew Viterbi [1964]によるものです。スペクトラム拡散の歴史は、Robert Scholtz [1682]によって適切に伝えられています。スペクトル拡散の数学への古典的な紹介は、レイモンドピックホルツ、ドナルドシリング、ローレンスミルスタインによるものです[1525]。一方、標準的な教科書はRobert Dixon [567]によるものです。  
 ヒュー・グリスとニコラス・ウィリスは、第二次世界大戦[824]におけるRAFとドイツ空軍との間の電子戦争について説明し、R  
 ジョーンズのイギリスの電子戦争と科学的インテリジェンスの全体的な歴史は、技術がどのように開発されたかだけでなく、戦略的および戦術的な詐欺にも多くの洞察を与えます[990、992]。  
CarringtonイベントとEMPareに対する米国の電力網強化の不十分さは、MatthewとMartin Weiss [2005]によって議論されました。  
S  
S  
セキュリティエンジニアリング736ロスアンダーソン