戦争すべての戦争は欺瞞に基づいています...  
無秩序を見せびらかし、彼を粉砕します。  
– Thomas Hobbes  
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としても、コンピュータセキュリティとは別の主題でした。  
2007年のロシアのエストニアに対するサービス拒否攻撃は、多くの政策アジェンダにしっかりとそれを課しました。 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。  
元々は戦士のために開発された多くの技術が商用利用に適応されており、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衰弱したが、ロシアがその軍隊を近代化し、そしてAIがレーダー、ソナー、関連システム。  
電子戦は、サービス拒否攻撃（コンピューターセキュリティの人々が何年もの間無視してきたトピック）と、直接的な要因と心理的な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。  
  
昔ながらのコンピュータセキュリティは機密性、整合性、可用性についてのものでしたが、電子戦争ではこれとは逆のことが言えます。  
妨害、模倣、および物理的攻撃を含むサービス拒否。 2。  
これには、盗聴だけでなく、敵の電子システムの使用から運用上重要な情報を入手することも含まれます。  
それは、妨害に強いシステムの設計から、強力なマイクロ波攻撃に抵抗するための機器の硬化、対放射線ミサイルを使用した敵の妨害物の破壊まで、多岐にわたる。 •電子サポート。効果的な攻撃と保護を可能にするために必要なインテリジェンスと脅威の認識を提供します。  
これらの定義はSchleher [1662]から引用されています。  
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。  
 および電子インテリジェンス（Elint）  
前者はメッセージの内容とどのユニットが通信しているか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、後者は敵対的なレーダーやその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、知覚とターゲットの取得の精度を低下させるために、敵の認識を操作して敵を誤解させることです。  
 何をどのくらいの期間、そして欺瞞の標的が人間であるかについて、プライド、貪欲、怠惰、その他の悪徳を搾取することです。  
物理的な破壊は、ミックスの重要な部分です。一部の敵センサーと通信リンクは妨害（いわゆるソフトキル）によって無力化される可能性があります  
。  
電子兵器システムは、レーダー、赤外線、ソナーなどのセンサーがあるという点で他の兵器と同じです。センサーデータをコマンドアンドコントロールセンターに送る通信リンク。妨害装置、レーザー、ミサイル、爆弾などの出力デバイス。  
電子戦争が終わったら、情報戦争に引き継ぐ可能性のある教訓を見ていきます。  
23.3通信システム  
今日では、典型的なコマンドと制御の構造は、データ、音声、画像をサポートし、ポイントツーポイントリンクで動作し、ブロードキャス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。  
状況認識と部隊を指揮する手段がなければ、指揮官は効果がないと思われます。  
•1つの明白なタイプのトラフィックは、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。  
 送信されたメッセージの機密性と信頼性も同様です。  
•現場のエージェントなどの秘密資産との通信には、より厳しい要件があります。  
エージェントは、通信監視の結果として捕まるリスクを最小限に抑えるための対策を講じる必要があります。  
•HQとフィールドの小隊の間などの戦術的コミュニケーションもより厳しくなっています（ただし少し異なります）。無線方向の検出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、故意に虚偽のメッセージも問題である可能性があります。  
音声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航空機から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。  
 しかし、それは防御妨害システムを倒すために必要なパワーレベルと緊張しています。  
したがって、通信の保護には、状況に応じて、コンテンツの機密性、信頼性、トラフィック分析と無線方向探知への耐性、およびさまざまな種類の妨害への耐性のいくつかの組み合わせが必要になります。  
たとえば、1980年代初頭に東ヨーロッパの反体制組織が使用するように設計された1つのラジオは、通常はボイスオブアメリカとBBCワールドサービスが通常使用するラジオ帯域で運用され、ロシア人によって日常的に妨害されていました。  
攻撃には、一般に、目的が分析や方向探知ではなく単にサービス拒否である場合でも、テクニックの組み合わせが必要です。  
これはゲリラ戦争でも当てはまります。マラヤ、ケニア、キプロスでは、反政府勢力がなんとかして電話システムを劣化させ、警察に無線網の設置を強制した[1380]。  
、80年代。  
もちろん、軍の指揮系統を攻撃することははるかに古いです。部下を撃つ前に将校を撃つことは基本的な常識です。  
23.3.1信号インテリジェンステクニック  
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、無線信号のカコフォニーと、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）  
これは、第二次世界大戦でワイヤレスオペレーターを最初に認識する方法の直接の子孫です。つまり、モールス符号[1224]を使用した方法です。  
 も重要です。  
したがって、スパイは、移動する前にメッセージを送信するまでに数分かかる場合があります。  
 2つのサイトで受信した信号の位相を比較することにより、疑わしい信号を正確かつ自動的に特定します。最近では、1秒以上の送信が何でもプレゼントになり得ます。  
差し迫った攻撃は、第一次世界大戦中に大幅に増加した無線メッセージによって、そして最近では国防総省へのピザ配達の増加によって合図されました。  
 誇張するのは難しいです。  
しかし、今世紀には、トラフィック分析は影から出てきて、主要な研究テーマになりました。これについては、セクション26.2.2で、法執行機関および諜報機関の監視のコンテキストで説明します。  
アリスのスパイ行為（または麻薬取引など）を疑う場合  
これにより、数十人の容疑者のリストが表示されます。  
この手順を2〜3回再帰的に実行すると、何千もの連絡先が蓄積されます。それらは雪だるまのように降りてきます。  
したがって、ボブ、カミラ、ドナルドがアリスの連絡先であり、ボブとカミラがイブと連絡を取り、ドナルドとイブがファーカーと連絡を取っている場合、これらの人々全員が容疑者と見なされる可能性があります。  
9/11以降、コバートコミュニティの検出は非常にホットなトピックになり、研究者はこの問題に対してあらゆる種類の階層的クラスタリングとグラフ分割の方法を試みました。  
そのような技術に関する標準的な参考文献は、Easley and Kleinberg [599]です。  
人々はいくつかの番号を持つことができ、それらは番号を共有します。  
（テロリストの独房を運営している場合、信号担当官は歯科医や医者などのアクティブな連絡先が多すぎて効果的に分析できない場所で仕事をする必要があります）  
また、電話番号を人に関連付ける何ら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。  
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を超えているため、犯罪者にとって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。  
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。  
これはエシェロンとして知られ、電話、ファックス、および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、辞書と呼ばれるコンピューターが通過するトラフィックを検索して、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を探しました。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基づいて行われました。  
世界中に100を超えるノードを持つ大規模な分散検索エンジンになっています。  
トラフィック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を説明した。  
たとえば、セクション2.2.1.9で私はOperation Socialistについて説明します。ここでは、GCHQがベルギーの電話会社をハッキングして、ベルギーを経由するサードパーティの携帯電話トラフィックと、ブリュッセルのEU機関の通信にアクセスしました。  
これは、攻撃のトピックに私たちをもたらします。  
23.3.2通信への攻撃  
人々はしばしば「コードブレイキング」の観点から話しますが、これは非常に単純化しすぎです。  
ほとんどの本番攻撃は、機器または主要な素材の供給または管理に向けられています。  
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開示しました。これにより、何百万ものSIMカードのキーが危険にさらされ、インテリジェンスコミュニティが数百万の携帯電話のトラフィックにアクセスできるようになりました。  
輸出規制と同様に、これは明白である可能性があります（セクション4.3.1および26.2.9を参照）  
 およびVPN（セクション2.2.1.7）  
そのような活動は、「暗号化を可能にする」として政府機関によって知られ、彼らの予算は9つの図にあります。  
最近では、クラウドサービスプロバイダーや人事管理局などの主要な資産に対する中国の攻撃（本質的にすべての米国政府職員のクリアランスデータファイルを入手した）がセクション2.2.2で説明されています。  
戦術的な状況での目標は、多くの場合、ノードを検出して破壊すること、またはトラフィックを妨害することです。  
第二次世界大戦では、連合国はドイツのスピーカーを偽のコントローラーとして使用して、ドイツのナイトファイターに混乱を招く指示を送り、認証技術が発明されて敗北したため、知恵の戦いがありました。  
これらの目標間の妥協点を見つけるのは難しい場合があります。  
これによりops / intelの緊張が取り除かれるので、RDFに切り替えるか、保護されたリンクを適切に破棄します。  
、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。  
物理的な攻撃よりも効果的なケースには、衛星リンクが含まれます。この場合、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アップリンクが妨害されることがよくあります。  
（ボスニア戦争のセルビア情報戦争セルの中に、DDoS NATO Webサイトを狙った逸話がありました。）  
  
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、リンク層暗号化は無線では扱いにくいです。単独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ため、それだけでは必ずしも十分ではありません。  
これには、さまざまなテクノロジーが必要です。  
、低確率修正（LPPF）  
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、実現可能な場合は通常は最良です。  
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（両側で）引き続き使用されていました  
3番目のオプションはそれ自体が実質的な主題であり、これについては後で説明します（簡単に）  
多くのLPI / LPPF /アンチジャム技術は、スペクトラム拡散通信の一般名の下にあります。  
 バースト送信。  
 （GPSシステムの）高解像度の範囲から、他の多くの問題に適用されています  
これら3つのアプローチを順に見ていきます。23.3.3.1周波数ホッピング  
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、近くの対戦相手が能力のある装備を持っている場合、オプションはフォロワー妨害、つまり信号を観察して帯域内を追跡することです。通常は、連続する各周波数を単一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。  
。  
周波数ホッピングは、Bluetoothなどの民間アプリケーションで使用されており、低コストでまともなレベルの干渉堅牢性を提供します。  
対象の周波数帯域を掃引する信号分析レシーバーは、通常、それらを傍受します（関連する帯域幅、掃引速度、および滞留時間によっては、ホッピング信号を数回傍受する可能性があります）。  
周波数ホッパーは実装が簡単で、耐ジャム性のレベルが高いため、マンパック無線などの戦闘ネットワークで、ホップレートが毎秒50〜500の場合によく使用されます。  
高速ホッパー（理論上、ビットレートを超えるホップレートを持つと定義されています。実際には、ホップレートは1秒あたり10,000以上です）  
ホッパーは、私が行う手法よりも「LPI」が低い  
 次に説明します。スイープレシーバーを持つ相手が信号の存在を検出できるためです。また、低速ホッパーには、適切な広帯域受信装置を備えた対戦相手が信号を追跡できることが多いため、盗聴や方向探知に対してある程度の脆弱性があります。  
23.3.3.2 DSSS  
。  
この技法は、1938年の特許出願[1682]でスイスのエンジニアGustav Guanellaによって最初に説明され、1950年代に米国で広く開発されました。  
ホッピングと同様に、DSSSはかなりの妨害マージンを与える可能性があります（2つのシステムは同じ理論上のパフォーマンスを持っています）  
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、レーダーの範囲内に入ったとき）、LPIモードで作業することです。  
DSSSに関する大規模な文献があり、その技術は現在、コード分割多元接続（CDMA）として商業の世界で取り上げられています。  
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複雑です。  
1つの戦略は、ユーザーに参照信号を提供することで交代させることです。  
 あなたはこれを信頼するかもしれません。ただし、GPSを制御していない場合、同期攻撃を受け入れる可能性があり、GPS信号が妨害されている可能性があります。  
これにより、イギリスの戦車が裁判中に迷いました。  
現在、GPS妨害装置は商品アイテムなので、この章の後半で詳しく説明します。  
23.3.3.3バースト通信  
タイムホップとも呼ばれます。  
 ただし、DSSSよりも検出が困難な場合があります。デューティサイクルが低い場合、スイープレシーバはそれらを簡単に見逃す可能性があります。  
本当にハイグレードな部屋のバグはしばしばバーストを使用します。  
。  
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の送信を開始し、母親に返信します。  
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、流星の散乱を打ち負かすことは困難です。さまざまなLPI、LPPF、および妨害耐性機能と、フェージングやマルチパスへの耐性などのパフォーマンスの他の側面と、同時に対応できるユーザー数との間には、かなり複雑なトレードオフがあります。  
 とフォロワー。  
エンジニアリングのトレードオフもあります。  
一方、DSSS信号は、方向検出技術を使用して配置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キーマテリアルを抽出した対戦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が不可欠な場合があります。  
•NATSSで知られているように、DSSSとホッピングの両方がリンク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）としても知られています  
 [1662]。  
57.6KHzのデータレートと10MHzのチップレートのDSSS信号を持っています（つまり、36.5dBの妨害マージン）。  
ホッピングコードはすべてのユーザーが利用できますが、拡散コードは個々の回路に限定されます。  
1967年に開発が始まったGordon Welchmanは、第二次世界大戦中にブレッチリーでドイツの暗号も破っていました。 1970年代のパイロットプロジェクトの後、1980年代に本格的な開発が始まり、システムは2000年頃から完全に配備され、アフガニスタンとイラクでの使用が見られました[1956]。  
 静止軌道からの1度ビーム。  
ジャム保護はホッピングによるものです。そのチャネルは2GHz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。  
干渉のキャンセルなど、システムレベルのトリックもいくつかあります。これは、自分の無線で既知の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、ホップしたりすることができます。  
  
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。  
 は、湾岸諸国の民間インフラを広範囲に利用しました。衛星、無線リンク、専用線を使用して、短期間で巨大な戦術通信ネットワークが作成され、さまざまな米軍サービスの専門家は、通信能力の戦争への影響を主張しています決定的だった[942]。  
これは米軍のナビゲーションシステムとして始まり、ユーザーが関連する暗号化キーを持っていない限り、精度を約100ヤードに制限する選択的な可用性機能がありました。  
時が経つにつれて、GPSは民間航空で非常に有用であることが判明し、FAAは標準の軍用受信機の主張された8ヤードと比較して、選択的可用性を打ち負かし、約3ヤードの精度を提供する方法を見つけるのに役立ちました[630]。  
米国政府は、たとえばテロリストがGPSを使用していると思われる場合、GPSをオフにするか、エラーを導入する権利を留保します。  
ただし、やる気のある対戦相手を持つ多くのアプリケーションがあります。  
安価なデバイスは、通常5〜10mの短距離です。  
例は、位置Aで信号をサンプリングし、位置Bで再送信する計量化です（これは、ワームホール攻撃とも呼ばれます）。  
その結果、Bの近くの誰もが代わりにAの近くにいると思っています。  
。  
スプーフィングは、既知の場所にある別の受信機を基準点として使用する差分GPSを使用して主に検出できます（FAAのトリック）。  
これにより感度も向上し、現在の機器の大きなエラーの主な原因である都市の峡谷のマルチパスを扱います1。  
  
ターゲットの獲得と武器のガイダンスに関係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いるところです。  
 敵対的なターゲットを検出し、それらに武器を導く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。  
、そして依然として潜水艦戦争を支配している[846]。  
それは海上衝突防止装置として1904年に発明されましたが、その深刻な発展は1930年代にのみ発生し、第二次世界大戦のすべての主要な参加者によって使用されました[855、990]。  
  
配備された幅広いシステムには、捜索レーダー、消防レーダー、地形追跡レーダー、対撃砲レーダー、気象レーダーなどがあります。  
たとえば、RFが低く、パルス繰り返し周波数（PRF）が低いレーダー  
この技術に関する古典的な教科書はSchleher [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。  
 直接。  
多くのレーダーにはレンジゲートがあります。これは、アンテナから特定の距離範囲内にあるターゲットに焦点を合わせる回路です。レーダーがすべての物体を追跡する必要がある場合（たとえば）  
これは、一般的に角度分解能とトラッキングパフォーマンスに影響を与えます。  
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、相対速度が速すぎる車両を無視するようにゲート制御されたレーダーを使用します（そのため、対向車でパニックになりません）  
別の車が20mも離れていないあなたの前の近くに押し込んだ場合、クルーズコントロールはそのことに気づかず、減速しません。  
23.4.2妨害技術  
広く使用された最も初期の対策はチャフでした。これは、ターゲット信号の波長の半分にカットされ、分散されて偽のリターンを提供する導電箔の薄いストリップです。  
チャフは、防御装置を貫通しようとする航空機によって直接落下する可能性があります（その後、細長い信号の頂点にあるため、これは理想的ではありません）。  
チャフに対する主な対抗手段はドップラーです。チャフは非常に軽いので、ほぼ同時に静止し、動いているターゲットからかなり簡単に区別できます。  
 他のより価値のあるもの（空母など）のおとりとして機能します  
これらの原則は非常に一般的です。  
 赤外線誘導ミサイルはフレアを使用して方向転換されている間、誘惑RF信号を発する特別な無人偵察機によっておとりです。  
 非常に短い範囲でのみ検出できるように車両の。  
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RCSの側面を継続的に示すフライバイワイヤーシステムがあ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）。  
アクティブな対策ははるかに多様です。  
一部のシステムは、対象の周波数範囲を通過するパルス妨害波や掃引妨害波などの系統的な周波数パターンを使用しました（別名、スキージングオシレーター）  
しかし、そのような信号はブロックするのがかなり簡単です。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クにすることです。  
もう一方の端には、対放射線ミサイル（ARM）などのハードキルテクニックがあります。  
このような武器に対する防御には、おとり送信機、点滅送信機のオンとオフ、パッシブレーダーの使用が含まれます。これらは、ターゲットが跳ね返ったときにテレビやラジオ局などの既存の送信機からの信号を利用します。  
自己保護に使用されるほとんどの妨害装置は、何らかの詐欺の妨害装置です。弾幕とARM技術は、支援車両による使用により適している傾向があります。  
基本的なトリックは、逆ゲイン妨害または逆ゲイン振幅変調です。  
送信された信号を観察することでサイドローブ応答をマッピングでき、妨害波信号を生成して、正味の放射がアンテナの指向性応答の逆になるようにすることができます。  
逆ゲイン妨害は、古いコニカルスキャンファイアコントロールシステムに対して非常に効果的です。  
これはコヒーレントでない場合があります。その場合、ジャマーはトランスポンダと呼ばれ、コヒーレント、つまりリピータの場合は正しい波形になります。  
 信号処理を使用してそれらを操作します。  
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。  
。  
同様に、ドップラーレーダーの基本的なトリックは、速度ゲートプルオフ（VGPO）です。  
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。このようなフォロワーの妨害は、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。  
3つの対策は、レーダーが最初のリターンパルスにのみ応答するリーディングエッジトラッカーを備えることです。と（カウンター）  
代替案は、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。  
チャフは、レーダーをドップラーモードに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（ドップラーのパルスよりも連続波形の方が良いため）。  
たとえば、真のターゲットは変動し、現実的な加速を持ちますが、単純なトランスポンダとリピータは、ほぼ安定した信号を出力します。  
そして今、CPUは現実的な偽のリターンを製造するのに十分強力です。  
23.4.3高度なレーダーと対策  
パルス圧縮は、第二次世界大戦でドイツで最初に開発され、一種の直接シーケンススペクトラム拡散パルスを使用して、一致したフィルターによって戻り時にフィルターされ、再度圧縮されます。  
パルス圧縮レーダーは、トランスポンダジャマーには耐性がありますが、特にデジタル無線周波数メモリを備えたリピータジャマーに対して脆弱です。  
パルスドップラーはドップラーとほとんど同じで、一連の位相安定パルスを送信します。  
エレメンタリーパルストラッキングレーダーと同様に、RFとパルス繰り返し周波数が異なると、特性も異なります。範囲/速度を明確にし、乱雑さを減らすために、低周波数/ PRFが必要です。  
通常の妥協点は中程度のPRFですが、これは空中作戦における範囲のあいまいさの深刻さに悩まされています。  
利点は、パルスドップラーが、ジェットエンジンのタービンブレードによって提供される変調などの非常に特定の信号を区別できることです。  
モノパルスは最も人気のある技術の1つになりました。  
アイデアは、4つのリンクされたアンテナを使用して、干渉技術を使用して各戻りパルスから方位角と仰角のデータを計算できるようにすることです。  
多くの場合、推奨される防御戦略は、牽引式デコイを使用することです。  
ロッキードの「サイレント歩哨」システムにはエミッタがまったくありませんが、商業ラジオおよびテレビ放送信号の反射を使用して空中の物体を検出および追跡します[164]。システムをノックアウトするには、主要な民間インフラストラクチャーを破壊する必要があり、反対者は法的および宣伝上の理由でそうしないことを好むでしょう。  
パッシブロケーションは実際には1930年代にレーダーのパイオニアであるロバートワトソンワットに戻り、1942年にドイツ人が最初に使用したようです。 「ヒッチハイカー」）  
これが1944年に起こっていることにイギリスが気づいたとき、チェーンホーム信号はジッターされました[824]。  
デジタル無線周波数メモリやその他のソフトウェア無線技術の登場以来、攻撃と防御はより複雑になっています。  
サイモン・ヘイキンらは、昆虫を狩るときにソナーをインテリジェントに適応させるコウモリが使用する戦略と戦術を研究し、これを最初に無線に適用してスペクトルを効率的に使用し、次に2006年の重要な論文のレーダーに適用しました[872]。  
 スイッチをオンにすると、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。  
これは非協力的なターゲットと敵対的になります。  
  
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、赤外線にもかなり当てはまります。  
フレアはチャフのようなもので、ターゲットに対して急速に減速するため、攻撃者は速度または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範囲ではありません。それは、混乱を引き起こす速度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。  
 [175]。  
たとえば、レイピア防空ミサイルは、レーダーを使用して、視覚条件で光学的に追跡しながら方位角を取得しました。  
セクション17.8で説明したように、2つの警報システムを組み合わせると、一般に、誤報率または見逃した警報率のいずれかが改善され、他方は悪化します。攻撃者が船や航空機などの反撃に弱い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、ランダムな時間で短い「ルックスルー」期間、妨害装置をオフにすることです。  
冷戦中は、両側に高出力の専用装置を備えた専門の支援車両が必要になると予想していました。これにより、ある程度のエネルギーの戦いになります。  
妨害の全体的な影響（ステルス時）  
しかし、妨害マージンも重要であり、誰が最も多くの車両を持っているか、そして戦術は採用されています。また、認知システムへの移行により、教義が「敵の通信やレーダーネットワークがだまされていることに気付かずに微妙に混乱させる」ように変化しました[721]。  
23.5 IFFシステム  
敵か味方か（IFF）  
アメリカの航空機がイギリスの兵士を爆撃した事件は、特に両国の当局が技術的安全の確保とまた、両方の目的からそのような事件を隠蔽しようとして失敗した後、英国の戦争に対する国民の支持の喪失に大きく貢献した。政治的な恥ずかしさを最小限に抑えます。  
例えば裁判官12：5–6（私は生体認証の章の冒頭で引用している）を参照してください。  
第二次世界大戦では、フランスの抵抗が人々に「グルヌーユ」の発音を要求し、それができない人はドイツ人と推定されました。  
ドイツの飛行機は、無線事業者が挑戦したときにロールオーバーし、レーダー断面に「ブリップ」を作成しました。  
朝鮮戦争により、ジェット機とミサイルの両サイドが到着し、標的を視覚的に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4.3.3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。  
チャレンジまたは応答が長すぎる場合、レーダーのパルス繰り返し周波数（およびその精度）  
一連の12〜20のチャレンジを送信し、元の実装では、実際の応答と予想される応答の算術差によってオフセットされた位置に応答が画面に表示されました。  
チャレンジは集中アンテナを使用し、受信機は無指向性であるため、反射攻撃が防止され、MIG-in-the-middle攻撃がはるかに困難になりました。  
 これは、後方互換モードを備えたMark XIIAによって主に置き換えられましたが、2010年代の米国のサービスとNATO軍による開発努力の焦点であった新しいモード5でスペクトル拡散波形を使用します。  
ただし、実際の問題は空対地になりました。  
 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ではこれは25％に増加しました。  
連立政権はまた、異なる国のシステムのためにリスクを増大させます。  
しかし、湾岸戦争が起こったとき、まともなものが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購入されるのではなく、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、そして立法者が同盟国との技術的協力をブロックすることによって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（彼らが私たちの仕事と私たちの秘密を盗むのを止めてください）  
そしてNATOは幅広い同盟です。あるインサイダーが私に言ったように、「極度に米国とギリシャの両方の願望に応えるソリューションを進化させようとしている（たとえば）  
イラクでは少数のユニットが使用しているセクシーなシステムがいくつかあり、ヘルメットに取り付けられたモノクルの地図表示に、すべての兵士がお互いの位置をリアルタイムで重ね合わせて見ることができます。  
ビッグバンアプローチが試みられましたが、失敗しました。共同戦術無線システム（JTRS、発音「ジッター」）  
しかし、これは国防総省の最大の調達失敗の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、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も求めていました。 -and-control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、それがリード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度がさらに高まることにより、彼ら自身の能力がさらに取り残されることを望まなかった。  
米国の教義、「軍事革命」（RMA）  
ヨーロッパ人は、村を爆撃することによって村からの狙撃兵の発砲に自動的に反応すべきではないと主張しました。 10人の武装勢力を殺害するだけでなく、100人の民間人を殺し、数百人の彼らの親戚を反対側に集めます。  
その結果、デッドロックが発生しました。各国は国家的解決策を追求することを決定し、冷戦以降、相互運用性に関して実際の進展はありませんでした。  
米国の航空機が同盟軍の多くの兵士を正当に爆撃し、殺害したため、同盟関係は弱体化した。  
  
即興の爆発物装置（IED）に対抗するために、電子戦対策でかなりの努力がなされました。  
米国に対する最初のIED攻撃  
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。  
その結果、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。  
他の多くのナショナリストや反乱グループは、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ナショナリストまで、IEDを使用しています。  
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との戦いには合計約7,000のIEDが関与し、英国の防衛科学者に妨害に関する多くの経験を与えました。弾幕妨害装置がVIPカーに取り付けられたため、IEDが早すぎたり遅すぎたりします。  
イラクの電子環境は、ベルファストやパキスタン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放射能を放出し、部隊が交代するにつれて常に変化しました。  
バグダッドに数百人の海軍の電子戦の専門家が配備されたとき、連合軍は問題を乗り越え始めました。その後、連合の妨害活動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。  
2003年にはほとんどすべてのIEDが連合軍に死傷者を出しましたが、2007年までに平均で4つのデバイスが使用されました[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するため、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。  
23.7指揮されたエネルギー兵器  
イギリスの科学者は問題を研究し、これは実行不可能であると結論づけました[990]。  
原爆の到来とともに物事は変わり始めました。  
誘導電流が大きいと電磁パルス（EMP）が発生する  
核爆発が地球の大気内で発生する場合、EMPエネルギーは主に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（テストはこれまでにありません）。  
ガンマ光子は地球の大気に衝突する前に数千マイルも移動する可能性があり、イオン化して大陸規模のアンテナを形成する可能性があります。  
さらに言えば、シアトルからサンディエゴまで米国西海岸にあるほとんどの電子機器は、ソルトレイクシティの上空250マイルの爆風によって一掃される可能性があります。  
キャリントンイベント– 1859年に天文学者リチャードキャリントンによって観測された大規模な太陽フレア–は同様の混乱を引き起こしました。そのため、カリブ海まで南にオーロラが発生しました。  
ロンドンのロイドは後に、そのような事件の米国だけでの費用は数兆ドルにもなる可能性があり、そのような事件は1世代または2世代ごとに避けられないと推定した[917]。このため、重要な軍事システムは慎重に保護され、大規模なITサービス会社がデータセンターを世界中に分散させ、警告衛星を設置し、大規模な変圧器などの重要な資産を保護するために十分な運営を行っている電力会社が資金を投入しています。  
当時、アメリカはヨーロッパに「中性子爆弾」を配備していました-建物を破壊することなく人々を殺すことができる強化された放射線兵器。  
 周囲の人々に影響を与えずに。  
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でしょう。実際の損傷は、日常の電子機器に起こります。  
戦場で使用する場合、EMP兵器はトラックに搭載する必要はなく、標準の爆弾や砲弾に収めることが望ましい。  
米国は、IEDの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、デトネーションの前にアンテナを配備する必要があり、それでも、通常の電子機器にとって半径わずか数百メートルでは致命的です。  
EMPの真の重要性は、イランや北朝鮮などの原始的な核技術をもつ国々に脅迫兵器を与えることかもしれません。  
電子通信への大規模な攻撃は、北朝鮮（またはイラン）などの国よりも、電子通信に依存している米国や日本などの国にとって脅威です。  
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」に移りましょう。  
23.8情報戦争  
その人気は湾岸戦争1での運用経験によって後押しされました。  
攻撃には、妨害装置や対放射線ミサイルなどの標準的な電子戦技術の混合が含まれていました。コマンドセンターへの巡航ミサイル攻撃;イラクに忍び込み、砂漠から長い通信ケーブルを掘り出した特殊部隊による攻撃。伝えられるところによると、ハッキングトリックを使用してコンピューターと電話交換を無効にします。  
 この作戦は、空爆の最初の夜に連合軍の犠牲者をゼロにするという目標を達成した。  
2007年4月、情報戦争はエストニアでの出来事によって議題に押し戻されました。  
エストニアのコンピューター緊急対応チームは、問題を巧妙な専門性で解決しましたが、彼らの国家的リーダーシップはNATO条約を呼び出し、ロシアに対する米軍の援助を求めました。  
イスラエルとパレスチナのハッカーの間、およびインディアンとパキスタンの間でも同様の争いがありました。  
それにもかかわらず、NATOはタリンに情報戦センターを設置することで対応しました。セクション2.2.3で説明したように、1つの結果はタリンマニュアルでした。州間の対立[1664]。  
攻撃とは、人への傷害または物的損害を引き起こすことが合理的に予想される操作です。彼らは民間人ではなく、戦闘員とその兵站だけに向けられるかもしれません。攻撃は無差別ではなく地理的に制限されている必要があります。病院や礼拝所から原子力発電所まで、いくつかの目標は立ち入り禁止です。  
軍事組織と民間組織の両方が使用するインフラストラクチャは公平なゲームであり、「裏切り」は禁止されていますが、「戦争の始まり」は禁止されていません。  
とにかく情報戦争とは何でしょうか。  
採用すべき（情報兵器）  
Cynicsは、冷戦後の予算を維持しようとして、機関が何十年にもわたって行ってきたことの単なるリマーケティングであるとの見方をしました。  
これは非常に広範であり、ハッキングだけでなく、すべての電子戦とすべての既存の情報収集技術（Sigintから衛星画像、スパイまで）が含まれています。  
後の記事で、彼女はコソボ戦争を取り巻くプロパガンダと活動におけるネットの役割について論じた[540]。  
彼は、情報の優位性を「情報の流れを収集、処理、および流布する一方で、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、コンピューターのセキュリティ問題についての技術的な詳細はデニングほどではありませんが、情報操作の軍事的法理を定式化する最初の試みを述べています。  
23.8.1制御システムへの攻撃  
グリッドを倒すことは、核攻撃に相当するサイバーです。電力供給が停止すると、現代の経済の他のすべてもかなり停止します。  
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しようとする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米国の標準的な戦術でした。  
 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、これらのシステムが世界中で進化したため、認証をサポートしていないことに気づき、セキュリティ研究者は2000年代半ばに制御システムに注意を向け始めましたプライベートネットワーク–施設内の固定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。  
いたずらが原因の1〜2件の事故、および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トンを流出させた事件[7]の後、制御システムのセキュリティ調査が始まりましたコミュニティ。  
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、ノースアメリカン電気信頼性公社（NERC）  
 ブラックスタート機能を備えた発電機が基本情報のセキュリティコンプライアンスを備えている必要があるという標準。  
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ず、最終的に収益が下がったため、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というものでした[104]。  
変電所の主なベンダーは3つあり、1つがプロジェクトの元請業者になると、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4msの遅延要件があるため、これを行うことは困難です[731]。  
したがって、この調査プログラムの実際的な成果の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化することによって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、国内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。  
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。  
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、変電所から政府の建物のHVACに至るまで、世界中で約60,000の脆弱なデバイスが見つかりました。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では、犯罪グループによる制御システムのハッキングに対する持続的な有能な関心は検出されなかったため、そのような活動の大部分は国家によるものであると想定するのが妥当です。俳優またはそのプロキシ。  
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アイダホ国立研究所が、NSAとそのイスラエルの対応者がStuxnetワームを開発し、イランのウラン濃縮能力を損なったと報告されています2008〜2010年の期間。セクション2.2.1.11でこれを説明しました。  
 30件のウクライナの変電所を破壊し、230,000人を数時間暗闇に置いたサイバー攻撃による[2067]。  
他の制御システムへの攻撃がありました。明らかに、イランは2020年4月に農村部の給水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。  
23.8.2他のインフラストラクチャへの攻撃  
露骨な市場で取り扱える脆弱性に対して支払われた価格は急上昇し、脆弱性のあからさまな市場に加えて、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に彼らのアイデアを利用できる灰色の市場が開発されました。  
2007年のロシアのエストニアおよび2008年のジョージアに対する攻撃は、2008年のパキスタンによるYouTubeへの攻撃と同様に、ある程度心を集中させました（パキスタンは国内でのみサービスをブロックすることを計画していましたが、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）  
欧州ネットワークおよび情報セキュリティ機関（ENISA）  
BGPのセキュリティに関するセクション21.2.1で主な調査結果について説明しました。  
 それを教えてくれました。  
。  
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、Google、Facebook、Twitterなどの米国のサービスプロバイダーを除外して地元のチャンピオンを支持するという方針のため、中国はほとんど影響を受けません。  
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深く絡み合っているため、プーチン大統領は2019年5月にロシアのISPが11月までに外国のインターネットインフラストラクチャから独立して動作することを要求する法律を可決しました。  
それが機能するようになれば、中国と同様に、ロシアはインターネットに対する大規模な破壊攻撃を世界の他の地域で開始する可能性があります。  
23.8.3選挙と政治的安定への攻撃  
期間はアラブの春から始まりました。セクション26.4.1で詳しく説明します。  
セクション2.2.4で、アラブ政府が西側とイスラエルから監視技術に飛びついた方法を説明し、内外の敵を追跡して嫌がらせをするために元NSAの傭兵を雇いました。  
ロシアには管理選挙の長い歴史があります。  
その首長であるスタロボイトフ将軍は、古いKGBタイプであると報告されていました。彼の代理店はプーチンを彼の後継者に選んだエリツィン大統領に直接報告した。」 [733、1003]プーチン大統領の党が2007年に再選されるまでに、不正行為は非常に露骨になり、メディアの偏見が大きくなり、国の従業員が与党に投票するように命じられたため、国際社会は結果を無料で受け入れなかったそして公正。  
彼は2014年にウクライナを侵略し、同時にファシスト、同性愛者およびユダヤ人に対してそれを擁護すると主張し、クリミアを併合し、国際的な制裁をもたらした。  
ヨーロッパがウクライナへの侵入に対する罰としてロシアに制裁を課した後、クレムリンはヨーロッパ中の極右グループの主要な資金提供者となり、英国での英国離脱キャンペーンとドイツでのAfDなどの政党の台頭をサポートしました。  
制裁以降の全体的な戦略は、あらゆる手段で米国とEUを混乱させ、弱体化させることでした。  
プーチン大統領および他の権威主義的指導者は、偽のニュースで、国内外の多くのターゲットユーザーを圧倒します。この妨害は、より信頼性の高いメディアへの信頼を損ないます。そのメディアは、「偽のニュース」であると非難されます。  
もみ殻のようなバルクのおとりがあります。ロシア人が2014年にマレーシア航空のウクライナ上空のMH17を撃墜した後、彼らは多くの異なる陰謀論を並行して推し進めました[1593]。  
IFFを欺くのと同等のことは、三角測量である可能性があります。これは、対戦相手のブランドの主要な側面を盗む技術です（ボリスジョンソンがNHSをブレグジット国民投票の中心に据えたときのように）  
対放射線ミサイルに相当するのは、対戦相手のウェブサイトをブロックしたり、資金を乱暴にしたりすることです。  
したがって、選挙の安全性は匿名である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。  
 またはその後（鎧によって）  
成熟した民主主義国でも、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。  
これらの犯罪の開示は投票の再審議につながらなかった。英国の政治を3年間麻痺させただけでした。  
。  
今日に至るまで、多くの支持支持者は国民投票の結果を有効なものとして受け入れていません。これはロシア人の観点から見ると本当に素晴らしい成果です。繰り返しになりますが、ロシア人が果たした役割は、既存の分極化を悪用し、可能な場合は火にガソリンを投げることでした（たとえば、セクション2.2.3で説明したように、クリントンキャンプからハッキングされたメールを漏らすことによって）。  
クリントンが選挙に勝ったならば、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ハッキングされた選挙システムの証拠が現れたであろうと思います。  
選挙制度は警報のようなものです。セクション13.3で説明したように、アラームの信頼性を破棄してアラームを無効にすることができます。これにより、アラームは無視されます。  
トランプが2020年11月に勝利したか敗北したかにかかわらず、米国の有権者の間での二極化の増加と世界におけるアメリカの地位の低下が予想されます。これもロシアにとっての勝利です。  
彼らの焦点は、他の国に破壊的であれ政治的であれ、攻撃を行わずに、経済的、技術的、情報能力を構築することでした。  
これは、中国が米国の同業他社になることを目指しているために浮上している新しい冷戦のフロンティアになるように見えます。  
  
1999年に情報戦争にプロパガンダやその他の心理的作戦が含まれたことは、当時は少数派の見解でしたが、その後の出来事によって裏付けられてきました。  
ローマとモンゴルの無敵神話を宣伝する取り組みから、第二次世界大戦と冷戦の双方によるプロパガンダラジオ局の使用を通じて、コソボキャンペーン中のセルビアのテレビ爆破とチェチェンへのサービス拒否攻撃ロシアの機関によるWebサイト–ツールは変更される可能性がありますが、ゲームは変わりません。  
大きな盲点がいくつかありました。2016年のペンタゴンでは、サンクトペテルブルクの人々がBlack Lives Matterから来たふりをすることを心配するのは誰の仕事でもありませんでした[1221]。  
かつて、帰属は難しいと言われていました。それは裏付けられていません。  
さらに先進国の露出度は高く、サイバー攻撃が民間人を代替手段よりもはるかに標的とする場合、攻撃者は戦争犯罪者として描写される可能性があります。  
この本の第2版では、サイバー攻撃がオープン紛争とゲリラ戦のどちらで彼らの場所を見つけるのか疑問に思いました。  
イギリスやアメリカだけでなく、ドイツ、フランス、その他の国でも民主主義メカニズムへの攻撃が見られます。  
 または他の可能性はありますか？  
他には何があるの？  
   
電子戦争は冷戦の間に繁栄し、多くの興味深い技術を開発しましたが、そのいくつかは主流の情報セキュリティへの道を見つけました。  
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の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、国家の関係者が他の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との間には、いくつかの興味深い類似点があります。  
まず、敵対的な機械学習について見てきました。  
 計算に多くの労力を費やす迷彩を設計できますか？  
 次に、Cambridge Cyber​​crime Centreを介して、スパム、フィッシング、マルウェア、ボットネットのコマンドアンドコントロールトラフィック、およびその他のオンラインの不正行為に関する大量のデータを収集します。  
私たちは世界中の100人を超える研究者にデータのコレクションをライセンスしています。  
参考資料レーダーからステルス、EMP兵器に至るまで、電子戦の技術的側面に関する最高のオールラウンドリファレンスは、Curtis Schleher [1662]によるものです。良い要約はDoug Richardson [1601]によって書かれました。  
通信妨害の最も完全な参照は、Richard Poisel [1530]によるものです。  
V.  
[684]で、Santiago Figueroa-Lorenzo、Javier A〜norga、およびSaioa Arrizabalagaによって、産業用制御システムで使用され、調査されたさまざまなプロトコル、およびそれらの脆弱性が議論されました。情報操作に関するリーディングについては、心理学と監視に関する章の最後にリストしたリーディングをお勧めします。アメリカの民主主義へのロシアの攻撃のために  
上院[385]。