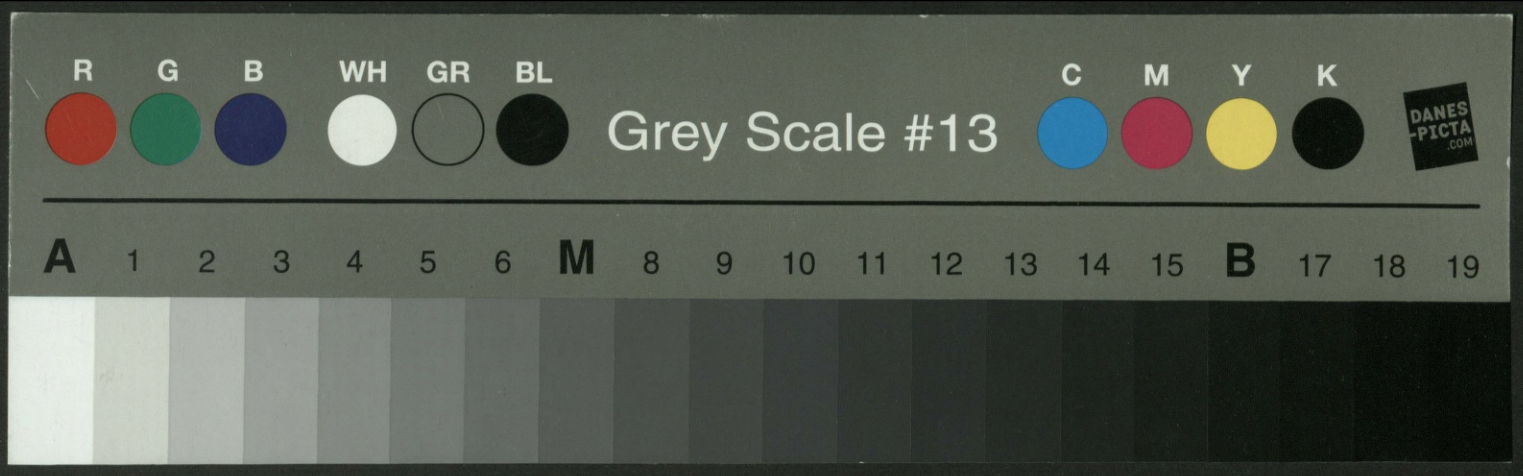
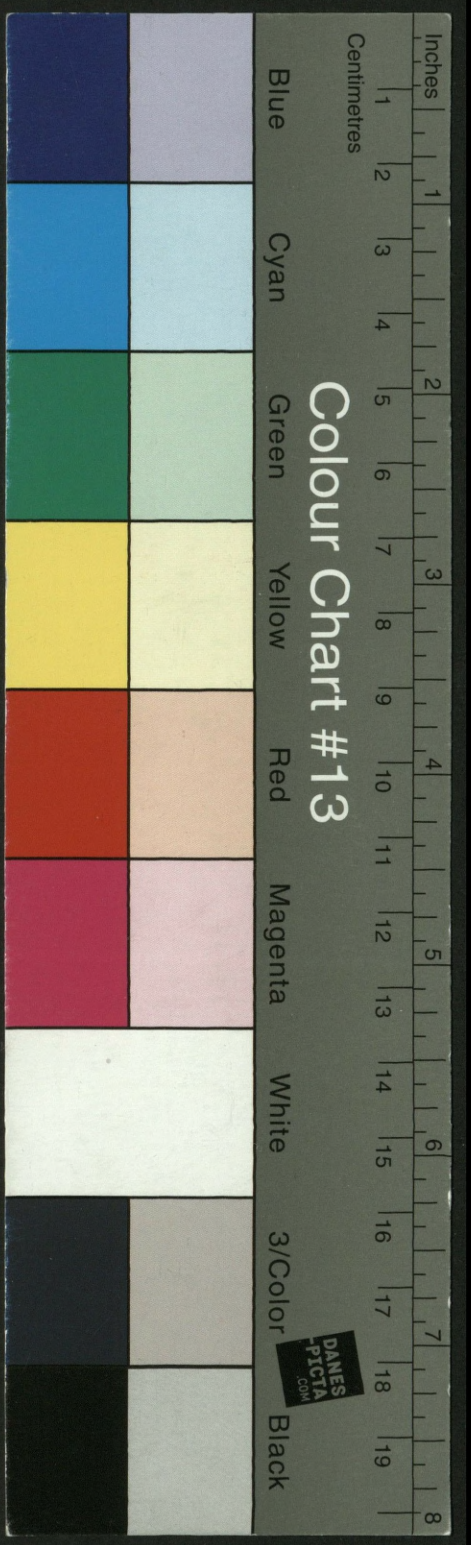




AKADEMIA OBRONY NARODOWEJ

Projekt badawczy 0500A 01923:
MODELOWANIE ZAGROŻEŃ DLA BEZPIECZEŃSTWA INFORMACYJNEGO PAŃSTWA. TEORIA WALKI INFORMACYJNEJ

ZAŁĄCZNIKI

WARSZAWA

AKADEMIA OBRONY NARODOWEJ

Projekt badawczy 0500A 01923:
MODELOWANIE ZAGROŻEŃ DLA BEZPIECZEŃSTWA INFORMACYJNEGO PAŃSTWA. TEORIA WALKI INFORMACYJNEJ

ZAŁĄCZNIKI

Warszawa 2004

Spis załączników

Załącznik 1

BEZPIECZEŃSTWO ELEKTRONICZNEGO PRZEKAZU DANYCH W SIECIACH TELEINFORMATYCZNYCH

Istnieje wiele niebezpieczeństw w dziedzinie przekazu danych w sieciach. By móc pisać o technikach ochrony danych należy najpierw sklasyfikować zagrożenia. Ataki na bezpieczeństwo można podzielić na:

- pasywne - napastnik po przechwyceniu wiadomości nie ingeruje w jej strukturę;
- aktywne - napastnik oddziaływuje na system informatyczny powodując przerwanie transmisji, modyfikację danych lub podszywa się pod kogoś innego.

Przykładem ataku o charakterze pasywnym jest **przechwycenie,** (rys.1 b).

Przykłady ataków aktywnych to:

Przerwanie, (rys.1c); zniszczenie części informacji albo spowodowanie jej niedostępności lub niemożności użycia - jest to atak na ***dyspozycyjność.***

Modyfikacja, (rys. 1 d); napastnik po zdobyciu zasobów dokonuje ich modyfikacji - jest to atak na ***nienaruszalność.***

Podrobienie, (rys.1 e); napastnik wprowadza do systemu fałszywe obiekty - jest to atak na ***autentyczność.***

Niezbędna również jest klasyfikacja usług ochrony:

Poufność to gwarancja, że informacje w danym systemie komputerowym lub przesyłane siecią mogą zostać odczytane tylko przez uprawnione osoby.

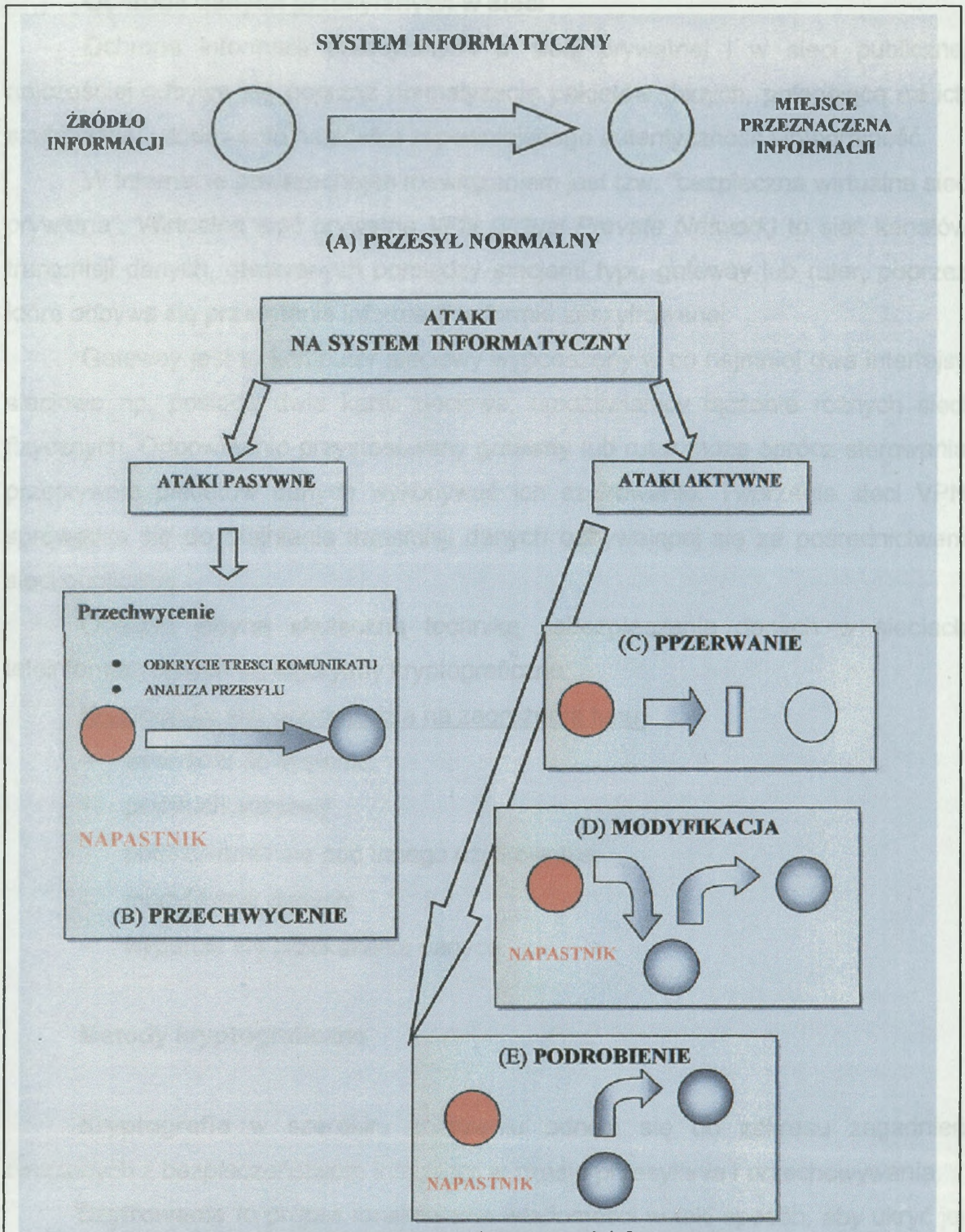
Uwierzytelnianie to gwarancja źródła. Polega na poprawnym określeniu pochodzenia komunikatu.

Nienaruszalność to gwarancja, że informacje w systemie mogą być modyfikowane, tylko przez powołane osoby.

Niezaprzeczalność transmisji jest to gwarancja, że ani nadawca, ani odbiorca nie mogą zaprzeczyć faktowi przesłania komunikatu.

Kontrola dostępu to gwarancja, że dostęp do źródła informacji jest kontrolowany przez system.

Dyspozycyjność to gwarancja, że uprawnione osoby będą mogły w każdej chwili korzystać z zasobów systemu.



Rys. 1. Aktywne i pasywne sposoby naruszania bezpieczeństwa w systemie informatycznym
Źródło: opracowanie własne na podstawie "Bezpieczeństwo systemów komputerowych" A. Grzywaka, Gliwice 2000

Ochrona danych przesyłanych w sieci

Ochrona informacji przesyłanych w sieci prywatnej i w sieci publicznej najczęściej odbywa się poprzez hermetyzację pakietów danych, polegającą na ich szyfrowaniu i dodawaniu nagłówka zapewniającego autentyczność i integralność.

W Internecie powszechnym rozwiązaniem jest tzw. "bezpieczna wirtualna sieć prywatna". Wirtualna sieć prywatna *VPN (Vrtual Prevate Network)* to sieć kanałów transmisji danych, otwieranych pomiędzy stacjami typu gateway lub ruter, poprzez które odbywa się przesyłanie informacji w formie zaszyfrowanej.

Gateway jest to komputer sieciowy wyposażony w co najmniej dwa interfejsy sieciowe np. posiada dwie karty sieciowe, umożliwiający łączenie różnych sieci fizycznych. Odpowiednio przystosowany gateway lub ruter może oprócz sterowania przepływem pakietów danych wykonywać ich szyfrowanie. Tworzenie sieci VPN sprowadza się do utajniania transmisji danych odbywającej się za pośrednictwem sieci publicznej.

Obecnie jedyną skuteczną techniką zabezpieczania danych w sieciach teleinformatycznych są algorytmy kryptograficzne.

Kryptografia jest odpowiedzią na zagrożenia typu:

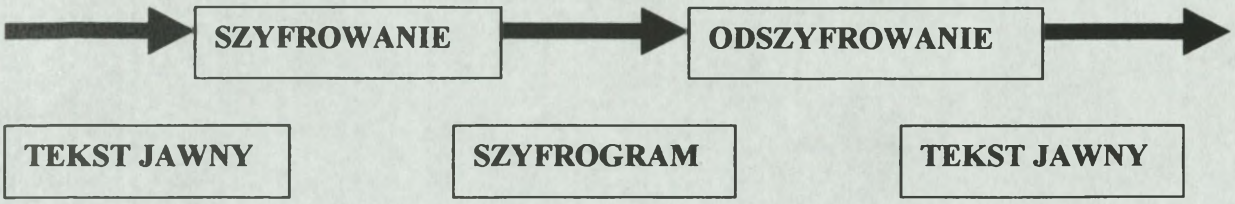
- włamania do systemu;
- podsłuch sieciowy;
- podszywanie się pod innego użytkownika;
- modyfikacja danych;
- wyparcie się przekazania danych.

Metody kryptograficzne

Kryptografia w szerokim znaczeniu odnosi się do zakresu zagadnień związanych z bezpieczeństwem informacji w czasie przesyłania i przechowywania.

Szyfrowanie to proces maskowania wiadomości w taki sposób, aby ukryć jej treść. Szyfrogram to treść informacji uzyskanej w wyniku szyfrowania.

Proces odszyfrowania czyli odczytania treści szyfrogramu rozpoczyna się od informacji przeznaczonej do szyfrowania nazywanej tekstem jawnym lub tekstem otwartym.



Rys. 2. Odczytanie szyfrogramu.

Szyfrowanie i odszyfrowanie odbywa się przy udziale algorytmu kryptograficznego, nazywanego również szyfrem, który jest w istocie funkcją matematyczną. W przeszłości bezpieczeństwo algorytmu było oparte na utrzymaniu w tajemnicy istoty jego działania. Takie szyfry nazywamy algorytmami ograniczonymi. Odegrały one istotną rolę w historii kryptografii. Obecnie nie zapewniają dostatecznego poziomu bezpieczeństwa.

We współczesnej kryptografii implementuje się systemy kryptograficzne ogólnego stosowania. Ich bezpieczeństwo nie jest warunkowane tajnością algorytmu szyfrującego i deszyfrującego lecz zależy ono od tajnego klucza deszyfrującego. Głównym celem kryptografii jest utrzymanie w tajemnicy tekstu jawnego.

Działaniami stojącymi w opozycji do kryptografii zajmuje się **kryptoanaliza**, nauka o odtwarzaniu tekstu jawnego bez znajomości klucza, bądź o odtwarzaniu klucza. Kryptoanaliza zajmuje się także wyszukiwaniem słabych punktów systemów kryptograficznych, które mogłyby otworzyć drogę do poznania tekstu jawnego.

Analiza bezpieczeństwa systemów kryptograficznych

Transmisja danych w transakcjach elektronicznych nie może przebiegać w warunkach zagrażających ujawnieniu lub jakiejkolwiek ingerencji w treść danych. Aby mieć pewność, że wiadomość zaszyfrowana nie zostanie ujawniona, należy zapewnić właściwe bezpieczeństwo klucza lub algorytmu szyfrującego. Bezpieczeństwo zapewnia również używanie algorytmów o odpowiedniej długości klucza tzn. takiej, która w znaczący sposób utrudni złamanie szyfru.

Szyfr jest bezwarunkowo bezpieczny, jeżeli generowany przezeń tekst zaszyfrowany nie zawiera informacji w ilości wystarczającej do tego, by określić jednoznacznie odpowiadający mu tekst jawny, niezależnie od ilości dostępnego tekstu zaszyfrowanego.

Szyfrem bezwarunkowo bezpiecznym jest szyfr z kluczem będącym losowym ciągiem znaków co najmniej tak długim, jak szyfrowana wiadomość i takim, że nie używa się tego samego klucza do szyfrowania innej wiadomości. Jeśli są spełnione powyższe warunki, to przeciwnik nie jest w stanie rozszyfrować tekstu zaszyfrowanego niezależnie od czasu jakim dysponuje, po prostu dlatego, że w tekście brak niezbędnych informacji.

Większość szyfrów jest jednak teoretycznie możliwa do złamania już przy znajomości kilkuset bitów treści jawnej[1]. Nie oznacza to jednak, że szyfry nie są dobrym zabezpieczeniem. Istotne jest czy szyfr jest bezpieczny pod względem obliczeniowym w sensie odporności na przełamanie, a nie bezwarunkowo bezpieczny.

Szyfr jest obliczeniowo bezpieczny, jeśli koszt złamania szyfru przewyższa wartość informacji zaszyfrowanej lub gdy czas potrzebny do złamania szyfru przekracza użyteczny „czas życia" informacji.

Systemy kryptograficzne jako klucze wykorzystują losowe ciągi znaków. Aktualnie w systemach teleinformatycznych dane są reprezentowane w postaci ciągów bitów. Kluczami są losowe ciągi bitów.

Systemy kryptograficzne dzieli się na dwie klasy:

- systemy o ograniczonym zasięgu;
- systemy ogólnego stosowania.

Bezpieczeństwo systemu o ograniczonym zasięgu wynika z utrzymania w tajemnicy algorytmu szyfrującego i deszyfrującego. W systemach ogólnego stosowania bezpieczeństwo nie zależy od tajności algorytmów, lecz od utajnienia klucza deszyfrującego. Przełamanie szyfru przy znajomości wyłącznie metody szyfrowania powinno być niemożliwe. Biorąc pod uwagę dostępność klucza szyfrującego wyróżnia się systemy kryptograficzne:

- prywatne – symetryczne;
- publiczne - asymetryczne.

Różnica pomiędzy publicznymi systemami kryptograficznymi a prywatnymi to problem utajniania klucza. Bezpieczeństwo systemów publicznych związane jest gównie z utrudnieniami jakie sprawiają obliczenia. Szyfrowanie powinno być obliczeniowo łatwe, deszyfrowanie również, ale tylko dla uprawnionego odbiorcy,

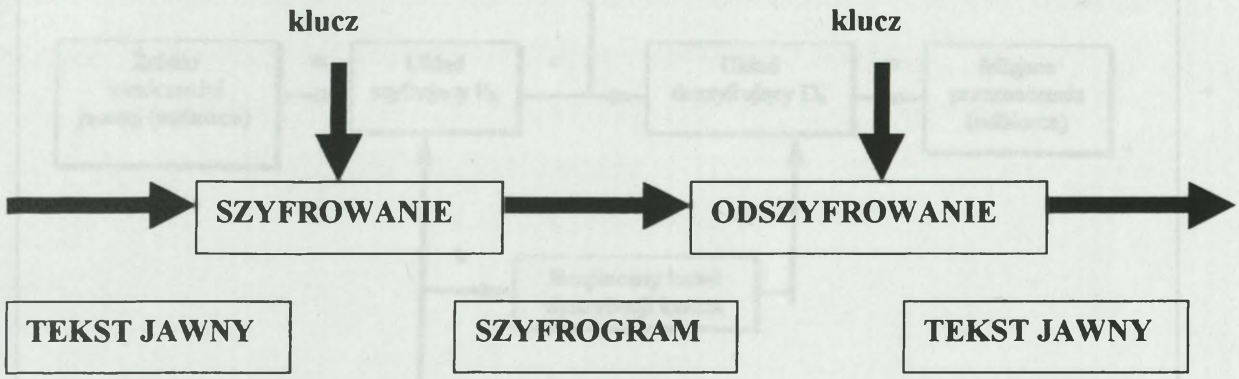
[1] *D. Elizabeth R. Denning „Kryptografia i ochrona danych" WNT Warszawa 1993*

trudne zaś dla odbiorcy nieupoważnionego. Szyfrowanie algorytmem publicznym jest asymetryczne, posługuje się dwoma oddzielnymi powiązanymi ze sobą kluczami, w przeciwieństwie do symetrycznego szyfrowania konwencjonalnego.

Prywatne systemy kryptograficzne

Algorytmy szyfrowania konwencjonalnego opierają się na dwóch zasadach. Po pierwsze na podstawianiu, gdzie każdy element tekstu jawnego jest odwzorowany na inny element. Po drugie na permutacji czyli przestawieniu kolejności elementów tekstu jawnego. Większość systemów przewiduje wiele etapów podstawiania i permutowania. Jest to łatwe do zrealizowania hardware'owo, ponieważ poszczególne bity doprowadzane są za pomocą połączeń w układzie na odpowiednie miejsca. Czas obliczeń permutacji odpowiada tu jedynie czasowi, w jakim informacje dotrą po połączeniach na miejsce przeznaczenia. Implementacja software'owa nie nadaje się ze względu na długie obliczenia, każdy bit oddzielnie musi być przekopiowany na miejsce przeznaczenia.

W kryptografii prywatnej algorytmy symetryczne charakteryzują się tym, że klucz szyfrujący jest wyznaczany z klucza odszyfrowującego i odwrotnie. W wielu przypadkach są one identyczne.



Rys. 3. Szyfrowanie i odszyfrowanie algorytmem symetrycznym
Źródło: „Bezpieczeństwo systemów komputerowych " Andrzej Grzywaka, Gliwice 2000

Formalne szyfrowanie i odszyfrowanie algorytmem symetrycznym można zapisać:

$$E(m)=c$$

$$D(c)=m$$

gdzie: **E** - funkcja szyfrująca;

m - tekst jawny;

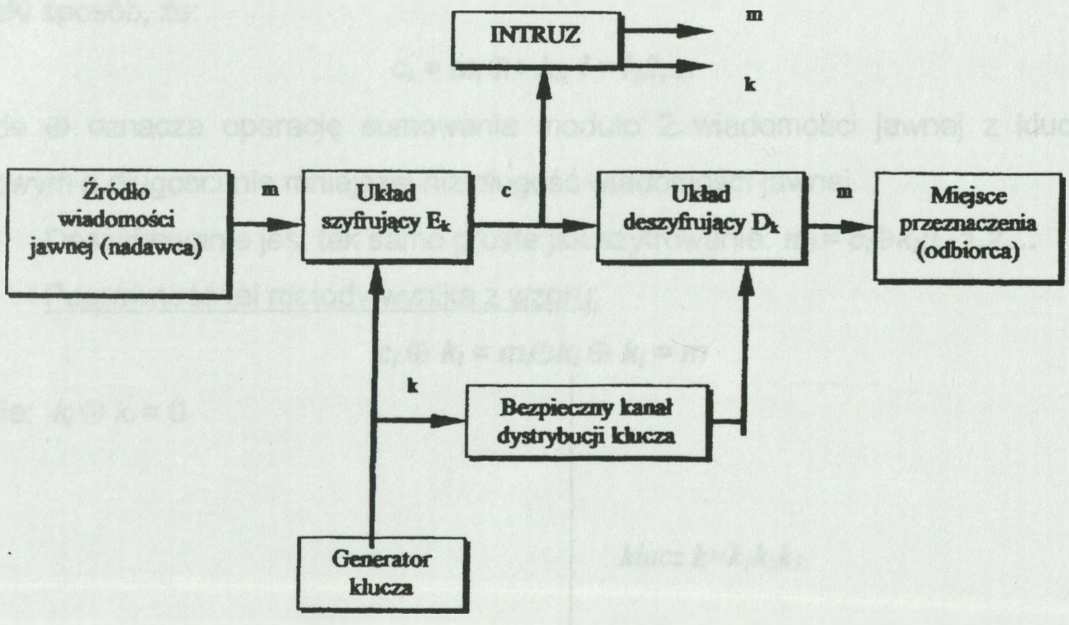
c – szyfrogram;

D - funkcja odszyfrowująca.

Algorytmy symetryczne wymagają uzgodnienia klucza pomiędzy nadawcą a odbiorcą, dlatego nazywamy je również algorytmami z kluczem tajnym. Algorytmy symetryczne dzielą się na dwie kategorie:

- **algorytmy strumieniowe** - przetwarzaną jednostką informacji jest jeden bit;
- **algorytmy blokowe** - przetwarzaną jednostką informacji jest grupa bitów, czyli blok.

Klucz szyfrujący i deszyfrujący są takie same. Bezpieczeństwo systemu zależy od tajności klucza i kanału dystrybucji klucza. Nie trzeba utajniać algorytmu, należy jedynie trzymać w tajemnicy klucz. Te cechy szyfrowania konwencjonalnego powodują, że jest ono powszechnie stosowane. Dzięki temu, że algorytm nie musi być tajny, producenci tworzą tanie realizacje sprzętowe algorytmów szyfrowania danych. Są one powszechnie dostępne i dołączone do wielu różnych produktów.



Rys. 4. Schemat blokowy prywatnego systemu kryptograficznego
Źródło: Opracowanie własne

Rys. 4. Schemat blokowy prywatnego systemu kryptograficznego

W przypadku, gdy alfabet wiadomości jawnej i alfabet wiadomości zaszyfrowanej są alfabetami języka naturalnego, można spodziewać się zjawiska redundancji (nadmiaru informacji). W sytuacji takiej istnieje możliwość skutecznej

analizy statystycznej tekstu. Aby udaremnić taką analizę stosuje się:

Konfuzję - utworzenie związku pomiędzy kluczem i szyfrogramem tak złożonego, jak jest to tylko możliwe. W rezultacie kryptoanalityk nie może uzyskać użytecznych informacji o kluczu na podstawie badań statystycznych szyfrogramu.

Dyfuzję - zatarcie statystycznych cech tekstu jawnego w kryptogramie. Można tego dokonać na dwa sposoby. Pierwszy to przestawienia - częstość występowania pojedynczych liter w szyfrogramie nie zostaje zmieniona, zaburzeniu ulega częstość występowania par liter, trójek itd. Drugi sposób to uzależnienie każdego znaku szyfrogramu od jak największej liczby znaków tekstu jawnego.

Szyfr bezwarunkowo bezpieczny to szyfr z kluczem będącym losowym ciągiem znaków, co najmniej tak długim jak szyfrowana wiadomość. Szyfr taki nazywamy jest szyfrem jednokrotnym. Szczególnym przypadkiem szyfru jednokrotnego jest szyfr Vernama. Przekształca on ciąg zerojedynkowy w ciąg zerojedynkowy[2].

Niech $m = m_1m_2...$ oznacza ciąg bitów tekstu jawnego, a $k = k_1k_2...$ ciąg bitów klucza. Szyfr Vernama generuje strumień bitów tekstu zaszyfrowanego $c = c_1c_2...$ w taki sposób, że:

$$c_i = m_i \oplus + k_i,\ i = 1,2,...$$

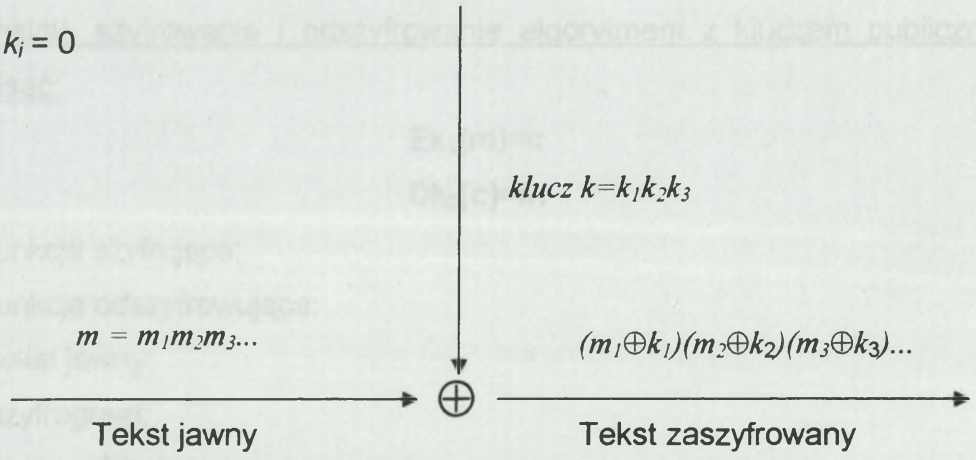
gdzie $\oplus$ oznacza operację sumowania modulo 2 wiadomości jawnej z kluczem losowym o długości nie mniejszej niż długość wiadomości jawnej.

Deszyfrowanie jest tak samo proste jak szyfrowanie: $m_i = c_i \oplus k_i; i = 1,2,...$

Poprawność tej metody wynika z wzoru:

$$c_i \oplus k_i = m_i \oplus k_i \oplus k_i = m$$

gdzie: $k_i \oplus k_i = 0$



Rys. 5. Szyfr Vernama

[2] *„Nauka" Encyklopedia Multimedialna PWN Warszawa 1999*

Do najbardziej rozpowszechnionych metod szyfrowania prywatnego zaliczamy:

DES (Data Encyryption Standard) - symetryczny algorytm szyfrowania z tajnym kluczem 56-bitowym, szyfrującym bloki 64-bitowe; opracowany przez IBM.

CAST-128 - stosuje klucz zmienny w zakresie 40 do 128 bitów.

IDEA (International Data Encryption Alghoritm) - międzynarodowy algorytm szyfrowania danych stanowiący rozszerzenie DES, z blokami 64-bitowymi i kluczem 128 bitowym.

Triple DES - algorytm symetryczny potrójnego szyfrowania DES z dwoma lub trzema różnymi kluczami. Wykorzystywany do szyfrowania kodów PIN przesyłanych między urządzeniami dokonującymi transakcje, a wydawcą karty.

RC2 - szybki algorytm szyfrowania, mający zastąpić DES.

RC4 - szyfrowanie kluczem zmiennej długości z operacjami bajtowymi, opartymi na losowych permutacjach.

RC5 - szybkie szyfrowanie ze zmiennym rozmiarem bloku i zmienną długością klucza (od 0 do 2048 bitów).

Publiczne systemy kryptograficzne

Algorytmy z kluczem publicznym stosują dwa klucze do szyfrowania i deszyfrowania. Klucz szyfrujący nazywany jest kluczem publicznym, ponieważ jest ujawniany. Do zaszyfrowania wiadomości może go używać każdy bez konieczności uzgadniania klucza. Odczytać zaszyfrowaną wiadomość może jedynie posiadacz klucza odszyfrowującego. Klucz odszyfrowujący nazywany jest kluczem prywatnym, utajnionym.

Formalnie szyfrowanie i odszyfrowanie algorytmem z kluczem publicznym można zapisać:

$$Ek_1(m)=c$$

$$Dk_2(c)=m$$

gdzie: **E** - funkcja szyfrująca;

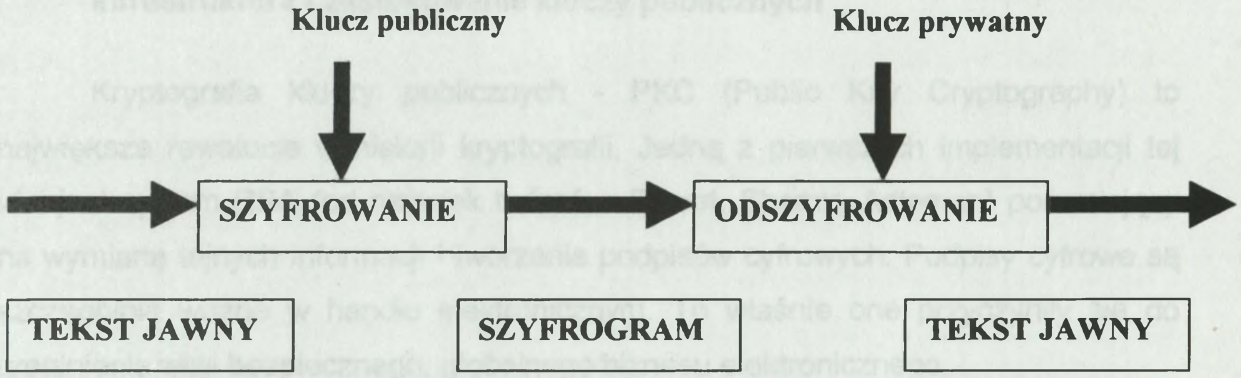
D - funkcja odszyfrowująca;

m - tekst jawny;

c – szyfrogram;

k_1 - klucz publiczny;

k_2 - klucz prywatny.



Rys. 6 Szyfrowanie i odszyfrowanie algorytmem z kluczem publicznym
Źródło: "Bezpieczeństwo systemów komputerowych " Andrzej Grzywaka, Gliwice 2000

W systemie publicznym każdy użytkownik otrzymuje od administratora systemu lub sam generuje tajny klucz ***k*** służący do deszyfrowania wiadomości. Klucz szyfrujący ***f(k)*** utworzony za pomocą funkcji zapadkowej ***f,*** podawany jest do wiadomości publicznej.

System szyfrowania publicznego jest asymetryczny, posługuje się dwoma oddzielnymi kluczami, które są matematycznie zależne.

Istotną cechą algorytmów publicznych jest niemożność określenia klucza prywatnego na drodze obliczeń, przy znajomości algorytmu kryptograficznego i klucza jawnego.

Główne etapy procesu szyfrowania z kluczem jawnym są następujące:

- każdy użytkownik w sieci generuje parę kluczy do szyfrowania i deszyfrowania otrzymywanych wiadomości;
- każdy użytkownik publikuje swój klucz szyfrujący (jawny) przez umieszczenie go w publicznym rejestrze lub pliku;
- w przypadku gdy nadawca chce wysłać wiadomość, szyfruje go za pomocą klucza jawnego odbiorcy;
- gdy odbiorca otrzymuje wiadomość, deszyfruje ją za pomocą prywatnego klucza.

Wszyscy użytkownicy mają dostęp do kluczy jawnych, klucze prywatne są generowane lokalnie przez każdego użytkownika.

Infrastruktura i zastosowanie kluczy publicznych

Kryptografia kluczy publicznych - PKC (Public Key Cryptography) to największa rewolucja w historii kryptografii. Jedną z pierwszych implementacji tej idei jest system RSA (od nazwisk twórców: Rivest, Shamir, Adleman) pozwalający na wymianę tajnych informacji i tworzenie podpisów cyfrowych. Podpisy cyfrowe są szczególnie ważne w handlu elektronicznym. To właśnie one przyczyniły się do urealnienia wizji bezpiecznego, globalnego biznesu elektronicznego.

Wraz ze wzrostem znaczenia Internetu w przeprowadzaniu transakcji biznesowych rośnie potrzeba zapewnienia ochrony informacji i właściwej identyfikacji stron uczestniczących w takich transakcjach. Wiele protokołów zapewniających poufność, integralność danych, uwierzytelnianie źródła danych oraz niezaprzeczalność wykorzystuje kryptografię z kluczem publicznym.

Zarządzanie kluczami oraz certyfikatami niezbędnymi dla tych protokołów zapewnia infrastruktura klucza publicznego.

Klucze publiczne są stosowane w szeroko rozpowszechnionych protokołach: SSL, SET i w podpisywaniu apletów Javy czy ActiveX, co stawia na pierwszym planie problem zarządzania zarówno tymi kluczami jak i certyfikatami.

Bezpieczna dystrybucja kluczy publicznych nierozerwalnie wiążę się z pojęciem certyfikatu cyfrowego. Certyfikat to strukturalny dokument kojarzący z kluczem publicznym pewien zbiór informacji i zaopatrzony w podpis cyfrowy zaufanej strony trzeciej, nazywanej Instytucją Certyfikującą - CA (Certification Authority).

Zarządzanie certyfikatami kluczy publicznych na skalę globalną jest przedsięwzięciem skomplikowanym. Trzeba zagwarantować wystarczającą liczbę wzajemnie połączonych sieci CA, zapewniających każdemu zainteresowanemu weryfikowanie dowolnego certyfikatu. Jak również system do wydawania i przechowywania certyfikatów, określenia ich autentyczności i unieważnienia certyfikatów w razie potrzeby. Ponadto w celu efektywnego użytkowania kryptografii kluczy publicznych i podpisów cyfrowych, potrzebne są inne usługi. Usługa niezaprzeczalności, cyfrowy notariat lub usługi cyfrowych datowników. Zespół takich usług tworzy infrastrukturę kluczy publicznych - PKI (Public Key Infrastructure).

Pierwszym krokiem w ustanawianiu PKI jest utworzenie systemu

uwierzytelniania. Jedna z metod uwierzytelniania to logowanie oparte na hasłach. Metodą bardziej bezpieczną są certyfikaty cyfrowe. Każdy certyfikat zawiera specyficzną informację identyfikującą użytkownika, obejmującą nazwę, klucz publiczny i unikatowy podpis cyfrowy, wiążący użytkownika z certyfikatem. Aby uzyskać certyfikat, użytkownik wysyła zlecenie do danego punktu rejestracyjnego - RA (Registration Authority), który weryfikuje jego tożsamość i prosi punkt certyfikujący - CA o wydanie certyfikatu. Certyfikat wydawany jest z datą ważności. Wydawanie i odwoływanie wymaga sprawnej koordynacji. To kolejna funkcja infrastruktury kluczy publicznych, działającej jako cała architektura obejmująca: zarządzanie kluczami, ośrodek rejestracyjny, ośrodek wydawania certyfikatów i zestawy różnorodnych narzędzi administracyjnych.

Funkcje systemu PKI

Funkcje rozwiniętych systemów PKI można ująć w kategoriach:

Generowanie kluczy - klucz prywatny i publiczny może być generowany lokalnie przez użytkownika lub przez CA (klucze mogą zostać dostarczone w zaszyfrowanym pliku albo w postaci fizycznej np. inteligentna karta).

Rejestracja - przed wydaniem certyfikatu dana jednostka przedstawia się CA bezpośrednio lub za pośrednictwem Urzędu Rejestracji (RA).

Certyfikowanie - proces, w którym CA wydaje certyfikat dla klucza publicznego danej jednostki.

Uaktualnianie kluczy - wszystkie pary kluczy muszą być regularnie uaktualniane, wydawane muszą być także nowe certyfikaty.

Składowanie i odtwarzanie kluczy - proces ten umożliwia przechowywanie kopii kluczy deszyfrujących wszystkich użytkowników. Kopia zapasowa prywatnego klucza może być przechowywana przez CA albo przez osobny system.

Obsługa cechy niezaprzeczalności - idea składowania i odtwarzania stwarza słaby punkt bezpieczeństwa systemu, dlatego para do szyfrowania danych może być składowana i odtwarzana, natomiast para używana do podpisu nigdy nie powinna opuszczać „posesji" użytkownika.

Certyfikowanie przechodnie - certyfikat wydawany przez jednego CA drugiemu CA. Certyfikat ten zawiera publiczny klucz CA związany z prywatnym kluczem CA służącym do podpisywania wydawanych certyfikatów.

Systemy zabezpieczeń to jedna z najbardziej dynamicznie rozwijających się technologii informatycznych.

Podsumowanie

Obecnie najskuteczniejszą techniką zabezpieczania danych w sieciach teleinformatycznych są algorytmy kryptograficzne. Kryptografia może być odpowiedzią na zagrożenia włamania do systemu, podsłuch sieciowy, modyfikacje danych, podszywanie się pod inną osobę a także wyparcie się wysłania danych.

Wyróżnia się dwa systemy kryptograficzne w zależności od dostępności klucza szyfrującego. Są to systemy prywatne i publiczne. Bezpieczeństwo współczesnych systemów kryptograficznych nie jest uwarunkowane tajnością algorytmu szyfrującego i deszyfrującego, lecz zależy od tajnego klucza.

Bezpieczeństwo systemów publicznych jest związane przede wszystkim z trudnościami obliczeniowymi szyfrowania i deszyfrowania. Szyfrowanie powinno być obliczeniowo łatwe, a deszyfrowanie łatwe tylko dla uprawnionego odbiorcy. W systemie publicznym każdy użytkownik otrzymuje od administratora systemu lub generuje sam tajny klucz służący do deszyfrowania wiadomości, natomiast klucz szyfrujący jest podawany do wiadomości publicznej. Zaszyfrować wiadomość przeznaczoną dla danego użytkownika może każdy, lecz odszyfrować może ją tylko on sam.

Bezpieczeństwo każdego systemu szyfrowania zależy od długości klucza i ilości pracy obliczeniowej. Nie istnieje nic co czyniłoby szyfrowanie prywatne lepsze od szyfrowania publicznego pod względem odporności na deszyfrowanie.

Załącznik 2

CHARAKTERYSTYKA ALGORYTMÓW SZYFRUJĄCYCH WYKORZYSTYWANYCH W PROCEDURACH BEZPIECZEŃSTWA W SIECIACH TELEINFORMATYCZNYCH

Techniki kryptograficzne są nierozerwalnie powiązane z metodami zabezpieczeń transmisji danych w transakcjach elektronicznych.

Celem tego rozdziału jest przedstawienie wybranych technik kryptograficznych.

Omówione zostaną tu najczęściej stosowane algorytmy:

Algorytm RSA, wykorzystywany między innymi do zabezpieczeń transmisji danych przez sieć przy dokonywaniu transakcji kartami kredytowymi oraz przy generowaniu podpisów cyfrowych.

Algorytm DES, mający zastosowanie podczas szyfrowania kodu PIN przy transakcjach przeprowadzanych w bankomatach i terminalach POS oraz stosowany do wyliczania kodu MAC na potrzeby uwierzytelniania komunikatu.

Algorytm RSA

Fundamentem RSA jest algorytm służący do generowania unikalnych i bezpiecznych par kluczy. Mnoży on dwie duże liczby pierwsze i z otrzymanego wyniku poprzez kilka innych dodatkowych operacji ustala klucz publiczny oraz zależny od niego klucz prywatny. Klucz publiczny służy do szyfrowania wiadomości i powinien być jak najszerzej propagowany. Klucz prywatny jest tajny i tylko przy jego pomocy można odszyfrować zakodowane wiadomości kluczem publicznym.

Szyfr oparty na algorytmie RSA korzysta z wyrażenia potęgowego. Tekst jawny jest szyfrowany blokami. Każdy blok ma wartość binarną mniejszą od pewnej liczby **n.** Szyfrowanie i deszyfrowanie dla bloku tekstu jawnego **m** i bloku tekstu zaszyfrowanego **c** mają postać:

$$c = m^e \bmod n$$

$$m = c^d \bmod n$$

gdzie: k_j **[e,n]** - klucz szyfrujący,

k_p **[d,n]** - klucz deszyfrujący.

Jeśli:

1) ed mod φ (n) = 1, gdzie φ jest funkcją Eulera,

2) m $\in$ {0,l,...,n-1}, przy czym nwd (m,n) = 1,

to:

$$(m^e \bmod n)^d \bmod n = (m^d \bmod n)^e \bmod n = m$$

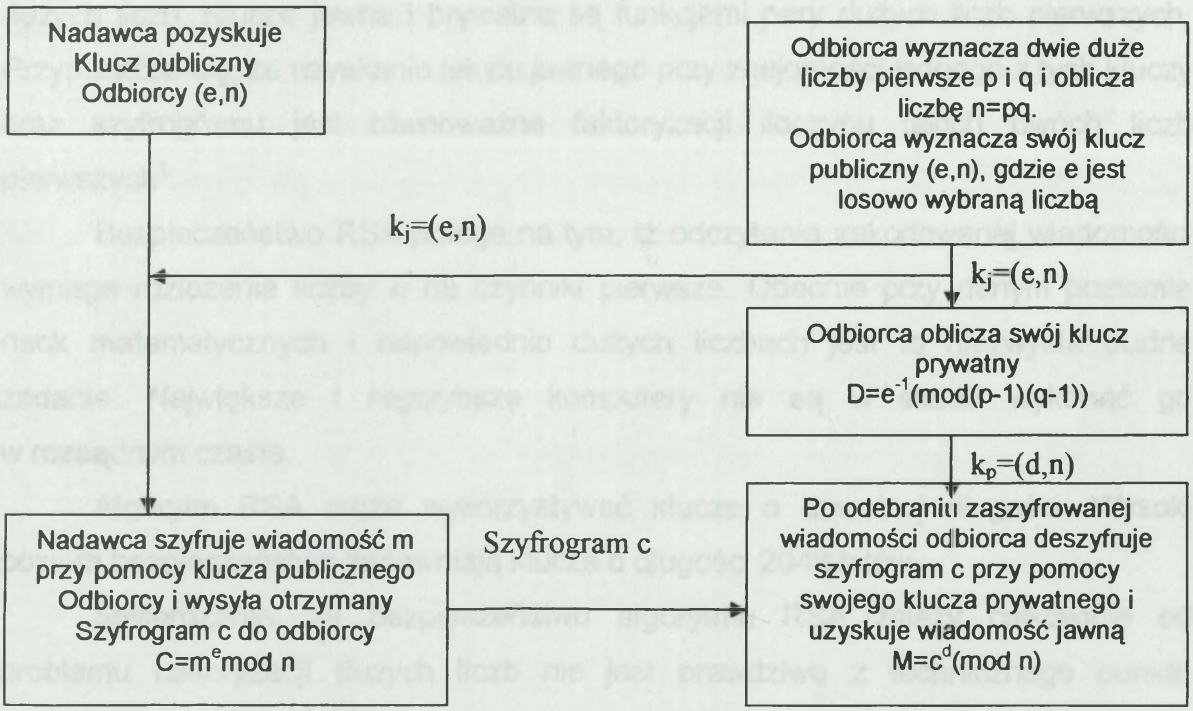
Skoro ed mod φ (n) = 1, to ed = r φ (n) + 1 dla pewnej liczby naturalnej r.

Korzystając z twierdzenia Eulera - Fermata otrzymuje się:

$(m^e \bmod n)^d \bmod n = m^{ed} \bmod n = m^{r\varphi(n)+1} \bmod n = m(m^{\varphi(n)} \bmod n)^r = m \bmod n = m$

oraz

$$(m^d \bmod n)^e \bmod n = m$$



Rys. 1. Koncepcja szyfrowania danych w algorytmie RSA

Bezpieczeństwo szyfrów potęgowych polega na dużej złożoności wyznaczania wartości logarytmów dyskretnych. Do wyznaczania kluczy w systemie RSA potrzebne są dwie losowo wybrane duże liczby pierwsze ***p i q.*** Na podstawie wyników znanych z teorii liczb uważa się, że powinny to być liczby około stucyfrowe. W rezultacie moduł ***n*** miałby około dwustu cyfr.

Nie wykazano jednak czy:

- złożoność obliczeniowa tego sposobu szyfrowania jest równoważna złożoności logarytmowania dyskretnego;
- moc algorytmu RSA jest równoważna rozkładowi liczby na czynniki pierwsze.

Istnieje jednak odmiana algorytmu RSA o złożoności takiej jak złożoność rozkładu liczby.

Bezpieczeństwo algorytmu RSA

Algorytm RSA wytrzymał lata intensywnej kryptoanalizy i obecnie nadal uważany jest za bezpieczny. Jego bezpieczeństwo wynika z trudności faktoryzacji dużych liczb. Klucze jawne i prywatne są funkcjami pary dużych liczb pierwszych. Przypuszcza się, że uzyskanie tekstu jawnego przy znajomości jednego z tych kluczy oraz szyfrogramu jest równoważne faktoryzacji iloczynu takich dwóch liczb pierwszych[1].

Bezpieczeństwo RSA polega na tym, iż odczytanie zakodowanej wiadomości wymaga rozłożenia liczby ***n*** na czynniki pierwsze. Obecnie przy danym poziomie nauk matematycznych i odpowiednio dużych liczbach jest to niezwykle trudne zadanie. Największe i najszybsze komputery nie są w stanie wykonać go w rozsądnym czasie.

Algorytm RSA może wykorzystywać klucze o dowolnej długości. Wysoki poziom bezpieczeństwa zapewniają klucze o długości 2048 bitów.

Stwierdzenie, że bezpieczeństwo algorytmu RSA zależy całkowicie od problemu faktoryzacji dużych liczb nie jest prawdziwe z technicznego punktu widzenia.

Wykazano, że odzyskanie nawet pojedynczego bitu z szyfrogramu otrzymanego przez zastosowanie algorytmu RSA jest tak trudne, jak odszyfrowanie całej wiadomości[2].

Wadą algorytmu RSA jest wolne działanie. Stosuje się go zazwyczaj w połączeniu z innymi algorytmami np. z DES, który operacje szyfrowania przeprowadza sto razy szybciej. W takich systemach hybrydowych DES służy do szyfrowania wiadomości, a RSA koduje klucz używany w DES-ie. Klucz zamknięty

---

[1] *B. Schneier „Kryptografia dla praktyków" WNT 1995*

w takiej elektronicznej kopercie może zostać bezpiecznie przesłany kanałem nie zapewniającym poufności np. przez Internet.

Algorytm DES

Algorytm DES jest algorytmem szyfru blokowego operującego na liczbach o długości co najwyżej 64 bitów. Blok 64 bitów tekstu jawnego wprowadzany jest na wejście algorytmu, na jego wyjściu otrzymujemy zaszyfrowany 64-bitowy blok danych. Ten sam algorytm jest wykorzystywany zarówno podczas szyfrowania jak i odszyfrowania. Jedyna różnica pomiędzy szyfrowaniem a odszyfrowaniem polega na odwrotnej kolejności podawania podkluczy podczas odszyfrowania. Algorytm wykonuje 16 cykli, podczas których wykonywane są dane operacje[3].

Funkcja szyfrowania przyjmuje dwa rodzaje danych wejściowych: tekst jawny do zaszyfrowania oraz klucz. Kluczem jest 64-bitowy ciąg (blok) zerojedynkowy ***k***, składający się z 8-bitowych bajtów, w których ósmy bit jest bitem parzystości. Klucz ***k*** służy do wytworzenia 48-bitowych pomocniczych kluczy szyfrujących $k_1, k_2, ..., k_{16}$. Na wstępie ciąg wejściowy ***k*** zostaje poddany permutowanemu wyborowi PSI i podzielony na dwa bloki, C_0 i D_0, zgodnie z tabelą 2.1.

Tabela 2.1.

Permutacja wyboru PSI

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Źródło: „ Bezpieczeństwo systemów komputerowych " Andrzej Grzywaka, Gliwice 2000

W kolejnych krokach ***i (i = 1, 2,...,1 f)*** bloki C_i oraz D_i uzyskuje się wskutek cyklicznego przesunięcia w lewo, odpowiednio, bloku C_{i-1} oraz D_{i-1} zgodnie z tabelą 2.2.

---

[2] *B. Schneier „Kryptografia dla praktyków" WNT 1995*
[3] *A. Grzywaka „Bezpieczeństwo systemów komputerowych" Gliwice 2000*

Tabela 2.2.

Przesunięcia połówek klucza C i D

Numer iteracji i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Liczba przesunięć w lewo	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Źródło:,, Bezpieczeństwo systemów komputerowych " Andrzej Grzywaka, Gliwice 2000

Klucz k_i uzyskuje się dokonując permutowanego wyboru PS2 według powyższej tabeli 2.3.

Tabela 2.3.

Permutacja klucza PS2

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Źródło: „Bezpieczeństwo systemów komputerowych" Andrzej Grzywaka, Gliwice 2000

Klucze pomocnicze $k_1, k_2, ..., k_{16}$ wykorzystuje się w procesie szyfrowania 64-bitowej wiadomości jawnej ***m***. Dokonuje się permutacji początkowej IP wg tabeli 2.4.

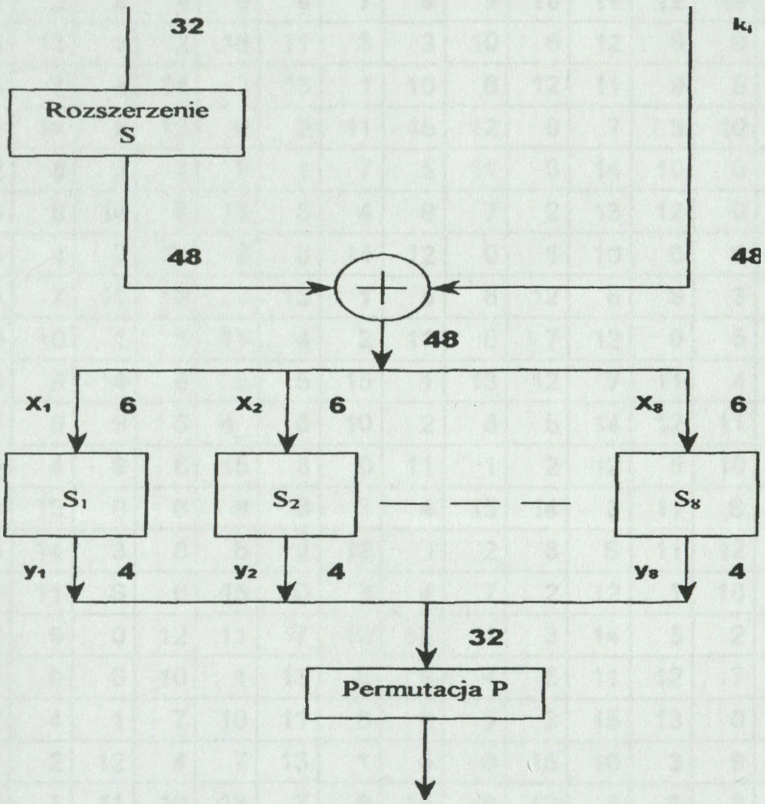
Tabela 2.4.

Permutacja początkowa IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Źródło: „Bezpieczeństwo systemów komputerowych" Andrzej Grzywaka, Gliwice 2000

Pierwszym bitem na wyjściu jest bit pięćdziesiąty ósmy wejścia, drugim – bit pięćdziesiąty itd., a bitem sześćdziesiątym czwartym - bit siódmy.



Rys. 2. Sposób wyznaczania wartości funkcji f.

Po dokonaniu permutacji początkowej IP są tworzone dwa 32-bitowe bloki L_0 *i* R_0, *a* następnie w szesnastu krokach dokonywane przekształcenia:

$$L_i = R_{i-1} \text{ oraz } R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$$

Przy czym $\oplus$ oznacza sumowanie modulo 2 odpowiednich bitów sumowanych bloków.

Wartość funkcji ***f*** (zależy od R_{i-1} i klucza pomocniczego k_i) wyznacza się zgodnie z zasadą przedstawioną na rys. 2 i w tabeli 2.5 -funkcje wyboru (skrzynki **S**).

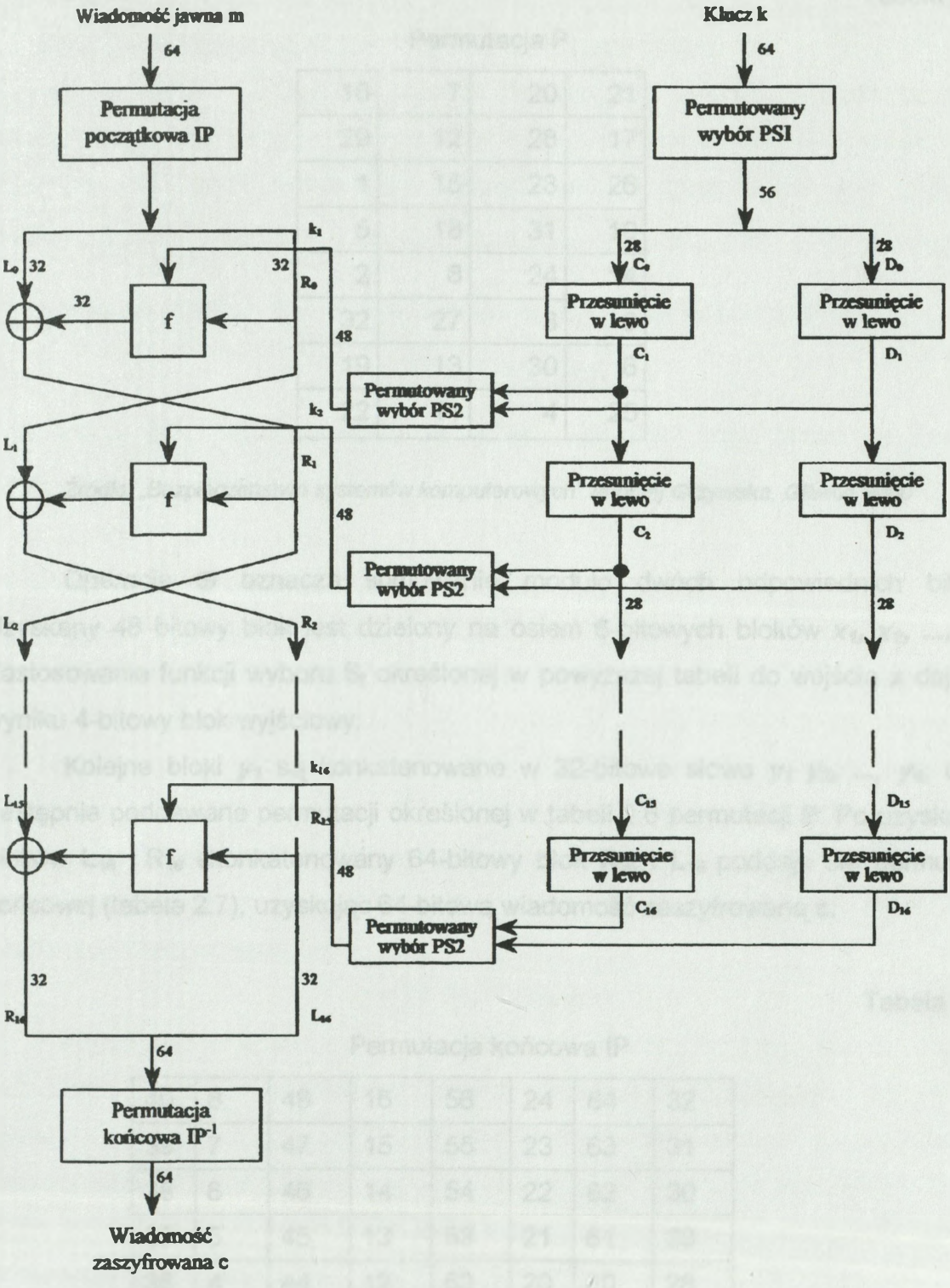
Jeśli $x_i = b_1,b_2,b_3,b_4,b_5,b_6$ to wartość $S_i(x_i)$ wyznacza się w taki sposób, że na przecięciu wiersza o numerze odpowiadającym postaci dziesiętnej liczby binarnej b_1b_6 *i* kolumny o numerze odpowiadającym postaci dziesiętnej liczby binarnej $b_2b_3b_4b_5$ odczytuje się $S_i\{x_i\}$ w postaci dziesiętnej; postać dwójkowa daje 4-bitową wartość $y_i = S_i(x_i)$.

Tabela 2.5.

Funkcje wyboru (skrzynki S)

	Kolumna																
Wiersz	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0	S_1
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10	S_2
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15	
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	
0	10	0	9	14	6	3	5	15	1	13	12	7	11	4	2	8	S_3
1	13	7	0	9	3	4_	6	10	2	8	5	14	12	11	15	1	
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7	
3	1	10	13	0	6	9	8	7	4	15	14	3	11	S	2	12	
0	7	13	14	3	0	6	9	10	I	2	8	S	11	12	4	15	S_4
1	13	8	11	S	6	15	0	3	4	7	2	12	1	10	14	9	
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4	
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14	
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9	S_5
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6	
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14	
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3	
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11	S_6
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8	
2	9	14	15	S	2	8	12	3	7	0	4	10	1	13	11	6	
3	4	3	2	12	9	5	15	10	I1	14	1	7	6	0	8	13	
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1	S_7
1	13	0	11	7	4	9	1	10	14	3	5	12	2	IS	8	6	
2	1	4	II	13	12	3	7	14	10	15	6	8	0	5	9	2	
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12	
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7	S_8
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2	
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8	
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11	

Źródło: „ Bezpieczeństwo systemów komputerowych " Andrzej Grzywaka, Gliwice 2000



Rys.3. Schemat blokowy algorytmu DES

Rozszerzenie bloku $R_{i=1}$ do słowa 48-bitowego R^*_{i-1} uzyskuje się w taki sposób, że jeśli $R_{i=1} = b_1, b_2, ..., b_{32}$ to:

$$R^*_{i-1} = b_{32}b_1b_2b_3b_4b_5b_6b_7b_8, \ldots, b_{28}b_{29}b_{30}b_{31}b_{32}b_1.$$

Tabela 2.6.

Permutacja P

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Źródło: „Bezpieczeństwo systemów komputerowych" Andrzej Grzywaka, Gliwice 2000

Operacja $\oplus$ oznacza sumowanie modulo dwóch odpowiednich bitów. Uzyskany 48 bitowy blok jest dzielony na osiem 6-bitowych bloków $x_1, x_2, ..., x_8$. Zastosowanie funkcji wyboru S_i określonej w powyższej tabeli do wejścia **x** daje w wyniku 4-bitowy blok wyjściowy.

Kolejne bloki y_1 są konkatenowane w 32-bitowe słowo $y_1\ y_2, ..., y_8$, oraz następnie poddawane permutacji określonej w tabeli 2.6 permutacji **P**. Po uzyskaniu bloków L_{16} i R_{16} skonkatenowany 64-bitowy blok R_{16} i L_{16} poddaje się permutacji końcowej (tabela 2.7), uzyskując 64-bitową wiadomość zaszyfrowaną **c.**

Tabela 2.7.

Permutacja końcowa IP

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Źródło: „Bezpieczeństwo systemów komputerowych " Andrzej Grzywaka, Gliwice 2000.

Pierwszym bitem na wyjściu jest bit czterdziesty wejścia, drugim - bit ósmy itd., a bitem sześćdziesiątym czwartym - bit dwudziesty piąty.

Szyfr DES operuje na zbiorze 64-bitowych ciągach reprezentujących wiadomości jawne i na takim samym zbiorze kluczy. Zbiór wiadomości jawnych jest taki sam, jak zbiór wiadomości tajnych, wobec czego DES jest szyfrem endomorficznym. Klucz $\mathbf{k} \in \mathbf{K}$ określa przekształcenie $\mathbf{DES_k: M \rightarrow C}$ i przekształcenie odwrotne $\mathbf{DES_k^{-1}: C \rightarrow M}$. Dla każdego $\mathbf{k} \in \mathbf{K}$ i dla każdego $\mathbf{m} \in \mathbf{M}$[4].

$$DES_k(m) = \overline{DES_{\bar{k}}(\bar{m})}$$

Przy czym $(\bar{m})$ oznacza słowo ***m*** (czyli skończony ciąg bitów), w którym zanegowano wszystkie bity.

Szyfrowanie wielokrotne

Algorytm DES posługuje się kluczem 64-bitowym. W rzeczywistości jest to klucz 56 bitowy, gdyż każdy ósmy bit jest bitem parzystości. Potencjalna liczba niezależnych kluczy algorytmu DES wynosi 2^{56}. W ataku polegającym na przeszukiwaniu wyczerpującym (testowanie każdego klucza po kolei) wystarczy przebadać 2^{55} kluczy, a średnio $2^{54} = 1{,}801439851 * 10^{16}$ kluczy. Najprostszy sposób zwiększenia klucza to dwukrotne szyfrowanie z dwoma niezależnymi kluczami k_1 i k_2. W przypadku gdy **m** jest wiadomością jawną, to szyfrowanie dwukrotne daje wiadomość zaszyfrowaną **c** w postaci:

$$\mathbf{c = DES_{k2}\,(DES_{k1}(m))}$$

Wyznaczenie zbiorów kluczy słabych i półsłabych oraz zbiorów kluczy palindromicznych i antypalindromicznych pozwala zabezpieczyć się przed sytuacjami, w których przy szyfrowaniu dwukrotnym wiadomość jawna pozostałaby niezmieniona albo zmieniona pozornie poprzez zanegowanie wszystkich bitów. Niech ***k*** i ***k**** będą kluczami odwrotnymi tj. takimi, że dla dowolnej wiadomości jawnej **m** spełniona jest zależność:

$$\mathbf{DES_k\,(DES_{k^*}(m)) = m}$$

Oznacza to, że jeśli zaszyfruje się wiadomość najpierw jednym kluczem, a potem drugim, to uzyska się wiadomość jawną.

---

[4] *J. Stokłosa „Algorytmy kryptograficzne" OWN Poznań 1994*

Tabela 2.8.

Klucze szyfrujące k i klucze odwrotne k*

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
k*	0	4	8	12	1	5	9	13	2	6	10	14	3	7	11	15

Klucze ***k(0), k(5), k(10), k(15)*** to klucze słabe, pozostałe to klucze półsłabe. Dla kluczy słabych **k = k*.**

Dla każdego **k**∈***{k(0), k(5), k(10), k(15)*** znalezienie takiego **x,** że:

$$DES_{k(i)}(x) = x$$

Wymaga wyczerpującego przeszukiwania w postaci 2^{64} prób, co jest obliczeniowo trudne. Można zmniejszyć liczbę prób korzystając z dalszych wyników. Z definicji kluczy odwrotnych wynika, że klucze pomocnicze są w relacji $k_i = k^*_{17-i}$; dla każdego $1 \leq i \leq 16$.

Rozpatrzmy sytuacje:

-$k_i = \underline{k_{17-i}}$ klucze są parami identyczne;

-$k = k_{17-1}$, odpowiednie bity klucza k_i są zanegowane bitami klucza $\underline{k_{17-i}}$.

W pierwszym przypadku słowo $k_1 k_2,\ldots,k_{16}$ *jest* palindromem, a **k** nazywa się kluczem palindromicznym. W drugim przypadku **k** nazywa się kluczem antypalindromicznym. Każdy słaby klucz jest palindromiczny i vice versa. Nie każdy jednak klucz półsłaby jest antypalindromiczny.

Klucze pomocnicze $k_1 k_2,\ldots,k_{16}$ klucza ***k*** algorytmu DES są w relacji:

-$k_i = \underline{k_{17-i}}$ wtedy i tylko wtedy, gdy k ∈ {k(0),k(5),k(10),k(15)};

-$k = k_{17-1}$ wtedy i tylko wtedy, gdy k ∈ {k(3),k(6),k(9),k(12)}.

Można wykazać, że:

1. istnieje dokładnie 2^{32} takich wiadomości x, że:

$DES_k(x)=x$ dla każdego k∈ {k(0),k(5),k(10),k(15)}.

2. istnieje dokładnie 2^{32} takich wiadomości x, że:

$DES_k(x)=\bar{x}$ dla każdego k∈ {k(3),k(6),k(9),k(12)},

Przy czym $\bar{x}$ oznacza słowo uzyskane ze słowa **x** po zanegowaniu wszystkich jego bitów.

Szyfrowanie dwukrotne byłoby zasadne, gdyby dla każdej pary kluczy (k_1,k_2) nie istniał taki klucz $\mathbf{k_3}$, że:

$$DES_{k1}(DES_{k2}(m)) = DES_{k3}(\mathbf{m})$$

- dla każdej wiadomości jawnej **m.**

Jeśli taki klucz k_3 istnieje to mówi się, że DES jest zamknięty ze względu na kompozycję przekształceń.

Schemat Tuchmana polega na trzykrotnym przekształceniu wiadomości jawnej **m:**

- zaszyfrowanie kluczem k_1;
- zdeszyfrowanie kluczem k_2;
- ponowne szyfrowanie kluczem k_1.

$$C = DES_{k1}(DES_{k2}^{-1}(DES_{k1}(m)))$$

DES jest czysty wtedy i tylko wtedy, gdy dla każdej trójki kluczy (k_1,k_2,k_3) istnieje taki klucz k_4, że:

$$DES_{k1}(DES_{k2}^{-1}(DES_{k3}(m))) = DES_{k4}(m)$$

DES nie jest ani czysty ani zamknięty.

W transakcjach elektronicznych algorytm DES stosowany jest według schematu Tuchmana. Klucz szyfrujący k jest 32-bitowy i traktuje się go jako dwie połówki 16-bitowe K_1, i K_r. Operacja enkrypcji wiadomości jawnej polega w tym przypadku na zaszyfrowaniu tekstu kluczem K_1, zdeszyfrowaniu kluczem K_r i ponownej enkrypcji kluczem K_1.

Wnioski

Algorytm RSA jako najpopularniejszy algorytm z kluczem publicznym wchodzi w skład wielu standardów i protokołów sieciowych. Jest często stosowany w komunikacji internetowej. Największe i najszybsze komputery nie są w stanie odczytać zakodowanej wiadomości algorytmem RSA. Wynika to z faktu, że odzyskanie nawet pojedynczego bitu z szyfrogramu otrzymanego przez zastosowanie algorytmu RSA jest tak trudne, jak odszyfrowanie całej wiadomości Wadą algorytmu RSA jest wolne działanie. Stosuje się go zazwyczaj w połączeniu z innymi algorytmami np. z DES, który szyfruje sto razy szybciej.

Algorytm DES tzw. Standard Szyfrowania Danych wykorzystywany jest w szyfrowaniu PIN kodu i numeru karty podczas transmisji danych w transakcjach bankomatowych i płatniczych.

Bezpieczeństwo współczesnych systemów kryptograficznych całkowicie zależy od klucza. Klucze kryptograficzne odgrywają bardzo ważną rolę w algorytmach kryptograficznych.

Załącznik 3

CERT POLSKA

Raport 2002

Przypadki naruszające bezpieczeństwo teleinformatyczne

1 Wstęp

1.1 Informacje dotyczące zespołu CERT POLSKA

CERT (Computer Emergency Response Team) Polska jest zespołem powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w sieci Internet. CERT Polska działa od 1996 roku (do końca roku 2000 pod nazwą CERT NASK), a od roku 1997 jest członkiem FIRST (Forum of Incidents Response and Security Teams). Od roku 2000 jest także członkiem europejskiej inicjatywy zrzeszającej zespoły reagujące – Trusted Introducer[1]. W ramach tych organizacji współpracuje z podobnymi zespołami na całym świecie.

Do głównych zadań zespołu należy:

- rejestrowanie i obsługa zdarzeń naruszających bezpieczeństwo sieci
- alarmowanie użytkowników o wystąpieniu bezpośrednich dla nich zagrożeń
- współpraca z innymi zespołami IRT (Incidents Response Team) w ramach FIRST
- prowadzenie działań informacyjno edukacyjnych, zmierzających do wzrostu świadomości dotyczącej bezpieczeństwa teleinformatycznego (zamieszczanie aktualnych informacji na stronie http://www.cert.pl/, organizacja cyklicznej konferencji SECURE)
- prowadzenie badań i przygotowanie raportów dotyczących bezpieczeństwa polskich zasobów Internetu
- niezależne testowanie produktów i rozwiązań z dziedziny bezpieczeństwa teleinformatycznego
- prace w dziedzinie tworzenia wzorców obsługi i rejestracji incydentów a także klasyfikacji i tworzenia statystyk

2 Statystyki CERT POLSKA

Zgodnie z powyższymi założeniami programowymi CERT POLSKA co roku przygotowuje i udostępnia statystyki dotyczące przypadków naruszenia bezpieczeństwa teleinformatycznego w polskich

[1] 22 listopada 2001 zespół uzyskał najwyższy poziom zaufania Trusted Introducer Accredited TeamLevel 2.

zasobach internetowych. Niniejszy raport jest siódmym z kolei raportem tego typu. Dotychczasowe (począwszy od roku 1996) raporty dostępne są na stronie CERT POLSKA (http://www.cert.pl/raporty)

3 Statystyka przypadków naruszających bezpieczeństwo teleinformatyczne[2]

3.1 Liczba przypadków naruszających bezpieczeństwo teleinformatyczne

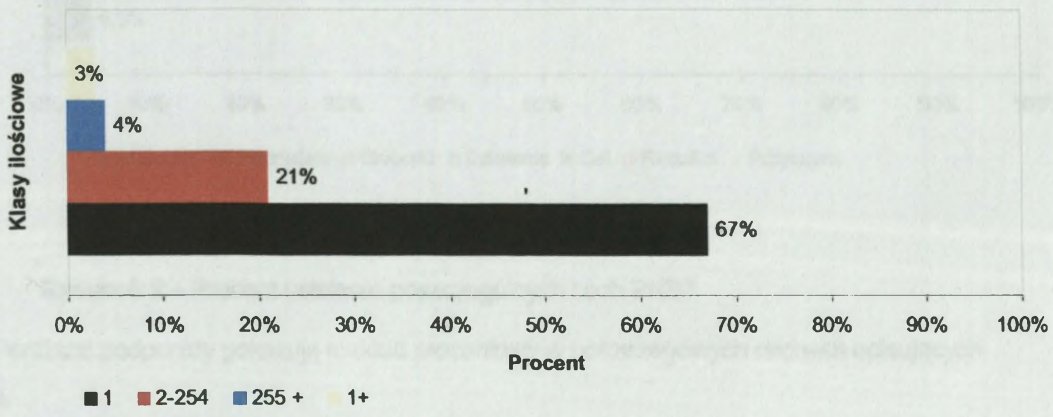
W roku 2002 odnotowano 3531 PNBT. Jednak 2518 przypadków było przypadkami tzw. spam'u (stanowi to 71,3% wszystkich przypadków). Przypadki te zostały potraktowane oddzielnie. Statystyki przedstawione poniżej odnoszą się więc do pozostałych 1013 przypadków.

3.2 Liczba zaatakowanych komputerów

Wśród stwierdzonych przypadków odnotowaliśmy takie, w trakcie których przeprowadzono atak na więcej niż jeden komputer czy inny obiekt sieciowy. W statystyce rodzajem „1+" określono te wszystkie przypadki, kiedy wiadomo było, że liczba zaatakowanych komputerów była większa niż jeden, jednak nie było możliwe ustalenie konkretnej wartości.

Mimo tego w 67% przypadków mieliśmy do czynienia z atakiem na jeden komputer.

W sumie nasze statystyki uwzględniły ataki na 107553 obiekty sieciowe[3].



[2] W dalszej części raportu przypadki naruszenia bezpieczeństwa teleinformatycznego określane będą skrótem PNBT lub terminem „przypadek"

[3] liczba ta uwzględnia jeden przypadek ataku na 65535 obiektów sieciowych.

Rysunek 1 - **Liczba zaatakowanych komputerów w trakcie jednego ataku**

3.3 Typy odnotowanych ataków[4]

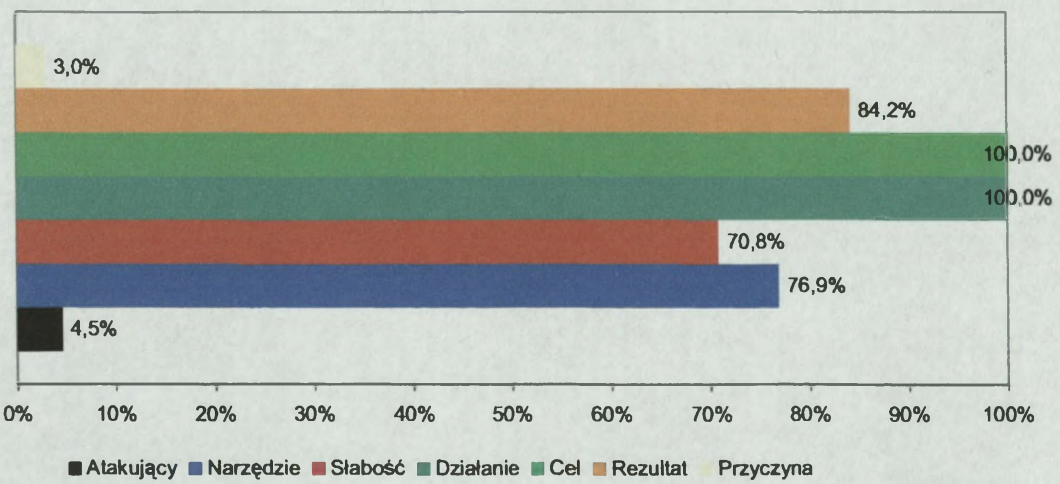
3.3.1 Klasyfikacja incydentów wg *Common Language*

Przypadki, w czasie obsługi których można było zgromadzić dane pozwalające na wypełnienie wszystkich cech przypadków, stanowią zaledwie 1,5% wszystkich przypadków.

Należy zwrócić uwagę, że klasyfikacja *Common Language* z założenia jest klasyfikacją kompletną, dlatego zawiera również kategorie, które właściwie nie są zupełnie zgłaszane do zespołów reagujących (np.: ataki fizyczne). Niemniej jednak dla porządku i pełnego obrazu, w naszych statystykach nie pomijamy tych kategorii.

Najbardziej podstawową formą ataku komputerowego jest tzw. zdarzenie (*ang. event*). Cechami charakteryzującymi *zdarzenie* są *działanie (action)* jakie podjął intruz oraz *cel (target)* jaki zaatakował. W związku z tym wszystkie przypadki muszą i mają określone te dwie cechy.

Poniższy wykres przedstawia w ilu przypadkach udało się ustalić daną cechę PNBT.



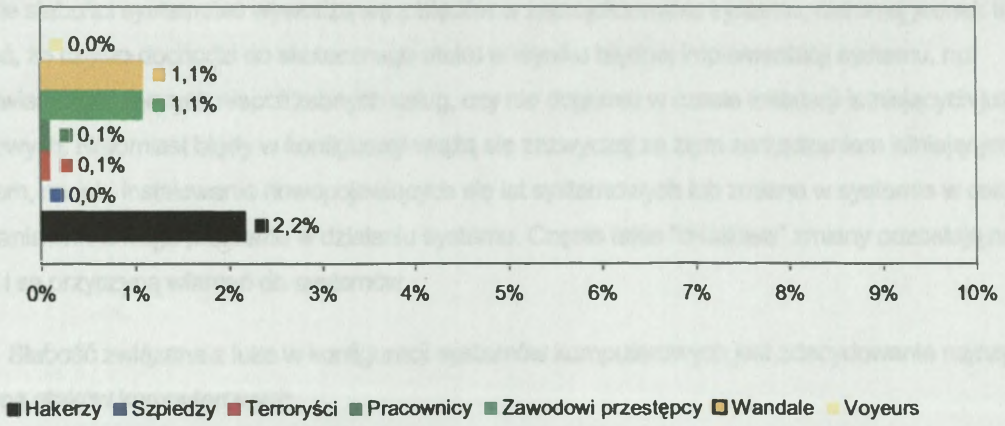
Rysunek 2 – Procent ustalenia poszczególnych cech PNBT.

Poniższe podpunkty pokazują rozkład procentowy w poszczególnych cechach opisujących przypadki.

[4] Począwszy od 2001 roku CERT Polska rozpoczął klasyfikację incydentów zgodnie z propozycją John'a D.Howard'a i Thomasa A.Longstaffa, znaną pod nazwą „Common Language" (*http://www.cert.org/research/taxonomy_988667.pdf*)

3.3.1.1 Atakujący[5]

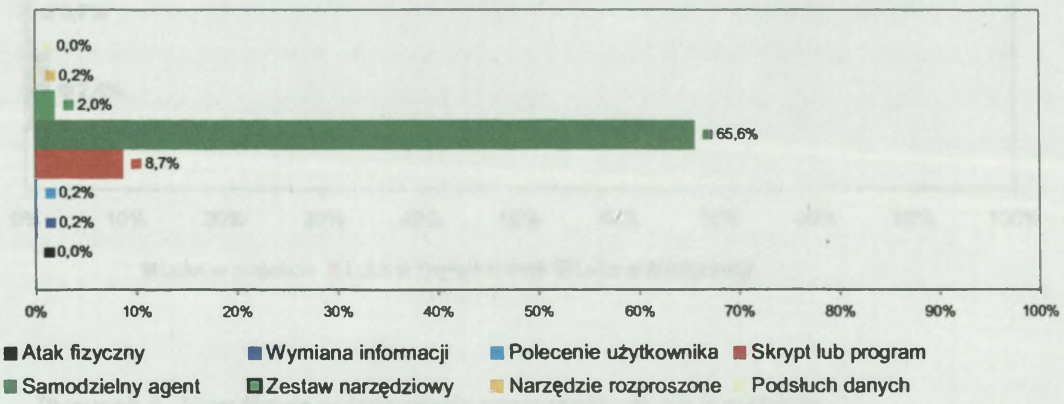
Na poniższym wykresie widzimy rozkład procentowy związany z kategorią „atakujący". Zgodnie z nim najczęściej do czynienia mieliśmy z hakerami, a w dalszej kolejności z wandalami i zawodowymi przestępcami. Należy jednak jeszcze raz zwrócić uwagę na niewielki procent ustalenia tej kategorii. Wyniki pochodzą z zaledwie 46 przypadków.



Rysunek 3 - Klasyfikacja atakujących

3.3.1.2 Narzędzia

Dla tej cechy związanej z PNBT zdecydowanie najwięcej jest przypadków, w których użyte zostały narzędzia określane jako „samodzielny agent". Jest to wyraźna kontynuacja trendu zapoczątkowanego w zeszłym roku, związanego z używaniem automatycznych narzędzi do ataków oraz działania na dużą skalę tzw. robaków internetowych. Oprócz znanych z roku 2001 robaków Code Red i Nimda w roku ubiegłym odnotowaliśmy bardzo wiele przypadków zainfekowania wirusem Klez.



[5] W tej kategorii nie zostało przetłumaczone pojęcie *voyeurs*, ze względu na jego specyficzne znaczenie i brak jednoznacznego odpowiednika w języku polskim.

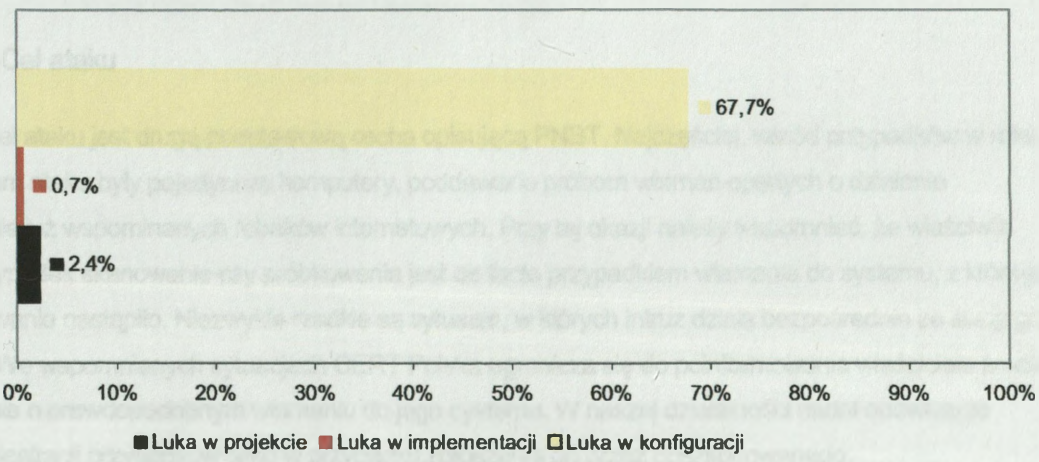
Rysunek 4 - Klasyfikacja używanych narzędzi ataku

3.3.1.3 Atakowana słabość systemu

Klasyfikacja *Common Language* wyróżnia trzy rodzaje słabości, które mogą zostać wykorzystane przez atakującego. Są to luka w projekcie, luka w implementacji oraz luka w konfiguracji. Poniekąd wszystkie słabości systemowe wywodzą się z błędów w zaprojektowaniu systemu, niemniej jednak trzeba pamiętać, że często dochodzi do skutecznego ataku w wyniku błędnej implementacji systemu, np: pozostawieniu działających niepotrzebnych usług, czy nie dograniu w czasie instalacji istniejących już łat systemowych. Natomiast błędy w konfiguracji wiążą się zazwyczaj ze złym zarządzaniem istniejącym systemem, np: nie instalowanie nowopojawiających się łat systemowych lub zmiana w systemie w celu rozwiązania chwilowego problemu w działaniu systemu. Często takie "chwilowe" zmiany pozostają na zawsze i są przyczyną włamań do systemów.

Słabość związana z luka w konfiguracji systemów komputerowych jest zdecydowanie najczęstszą przyczyną ataków komputerowych.

Naszym zdaniem jest to wynikiem coraz większego wpływu zarządzania bezpieczeństwem istniejących systemów, które często pozostają nieuaktualniane po początkowej, często nawet poprawnej, implementacji. Wszystkie najbardziej znane robaki i wirusy internetowe wykorzystują słabości systemowe, które już wcześniej zostały rozpoznane i dla których zostały stworzone łaty systemowe. Na usprawiedliwienie administratorów systemów, którzy są głównymi odpowiedzialnymi za taki stan rzeczy, należy dodać, że ilość słabości systemowych wykrywanych dla poszczególnych systemów stale rośnie[6] i skuteczne ich śledzenie oraz reagowanie na nie stało się dla większości nie lada wyzwaniem.



Rysunek 5 - Klasyfikacja wykorzystania poszczególnych luk w systemie

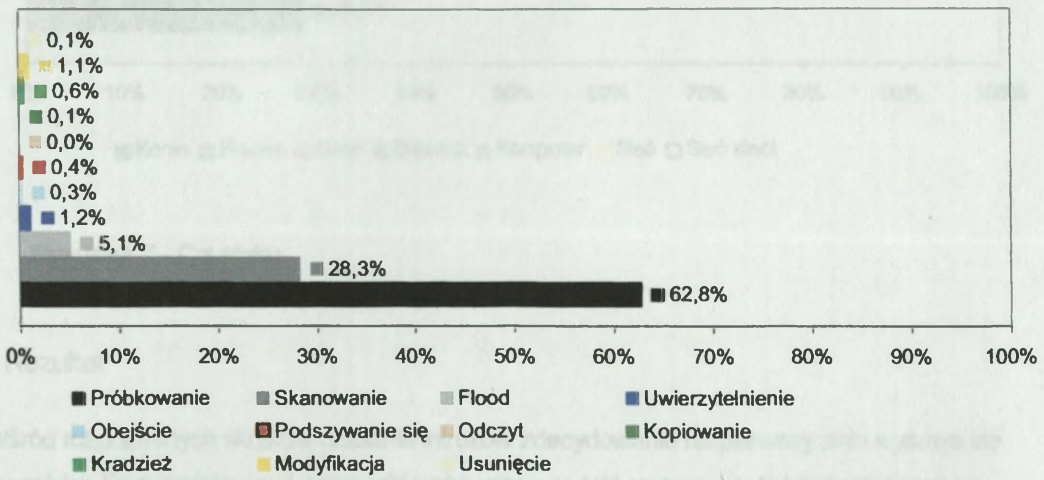
---

Voyeurs - *Atakujący, którzy atakują komputery dla podniecenia wywołanego uzyskaniem niejawnych informacji.*

[6] patrz: http://www.cert.org/stats/cert_stats.html#vulnerabilities

3.3.1.4 Nieautoryzowane działanie

Podobnie jak w roku ubiegłym zdecydowanie największy procent nieautoryzowanego działania stanowią przypadki próbkowania i skanowania. Wynik ten jest potwierdzeniem trendu, z którym mamy do czynienia od kilku lat. Zarysowała się wyraźna granica pomiędzy tymi, którzy są świadomi niebezpieczeństw związanych z używania Internetu a tymi, którzy nie będąc tego świadomymi stali się ofiarami tych zagrożeń, a ich komputery bardzo często pośrednikami w dalszych atakach. To właśnie ci pierwsi zgłaszają do CERT Polska incydenty, natomiast tych drugich to my sami powiadamiamy o odnotowanych przypadków i prawdopodobnych włamaniach do ich systemów.

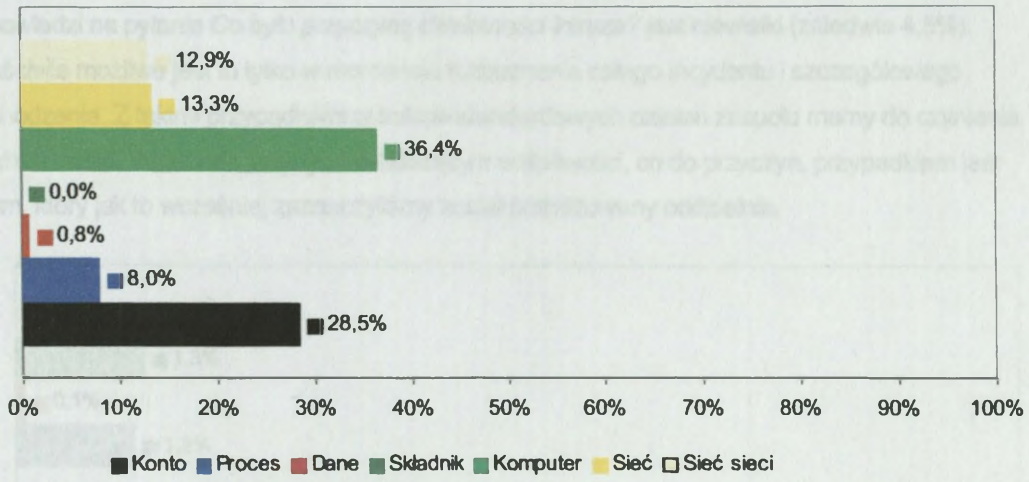


Rysunek 6 - Nieautoryzowane działanie podejmowane przez atakującego

3.3.1.5 Cel ataku

Cel ataku jest drugą podstawową cecha opisującą PNBT. Najczęściej, wśród przypadków w roku 2002, celem ataku były pojedyncze komputery, poddawane próbom włamań opartych o działanie wielokrotnie już wspominanych robaków internetowych. Przy tej okazji należy wspomnieć, że właściwie każdy przypadek skanowanie czy próbkowania jest de facto przypadkiem włamania do systemu, z którego to próbkowanie nastąpiło. Niezwykle rzadkie są sytuacje, w których intruz działa bezpośrednio ze swojego systemu. We wspomnianych sytuacjach CERT Polska ogranicza się do poinformowania właściciela źródła skanowania o prawdopodobnym włamaniu do jego systemu. W naszej działalności nadal obowiązuje zasada rejestracji przypadków tylko w przypadku zgłoszenia go przez poszkodowanego.

Atak na składnik jest w rzeczywistości atakiem fizyczny, np: kradzież tej części. Tego typu ataki jak dotąd nie są zgłaszane do CERT

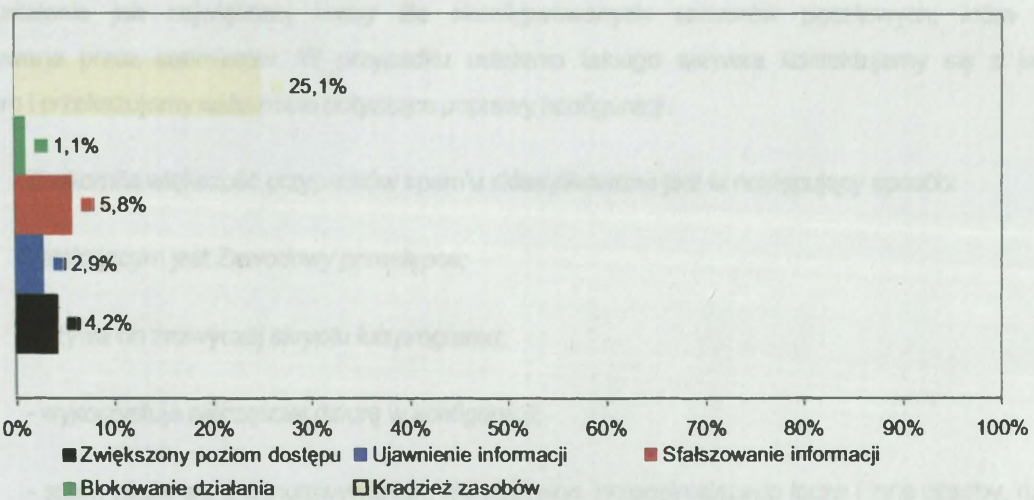


Polska.

Rysunek 7 - Cel ataku

3.3.1.6 Rezultat

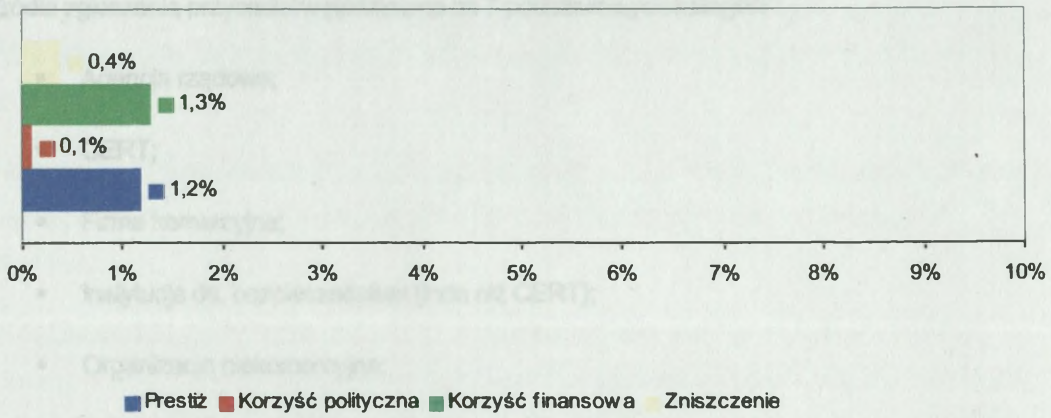
Wśród rozpoznanych skutków działania intruzów zdecydowanie na pierwszy plan wysuwa się *kradzież zasobów*. Dwa podstawowe przypadki wpływające na taki stan rzeczy to kradzież zasobów rozumianych jako moc obliczeniowa oraz rozumianych jak praca ludzka. Właśnie w przypadku skanowania mamy do czynienia z taką sytuacją. System poszkodowanego jest niepotrzebnie obciążony koniecznością „obsługi" nielegalnych pakietów a dodatkowo administrator musi poświęcić dużo pracy nad analizą logów ze swoich urządzeń filtrujących i systemów wykrywania zagrożeń.



Rysunek 8 - Rezultat przeprowadzonego ataku

3.3.1.7 Przyczyna

Przyczynę, która decydowała o wystąpieniu ataku jest bardzo trudno ustalić, dlatego procent odpowiedzi na pytanie *Co było przyczyną działalności intruza?* jest niewielki (zaledwie 4,5%). Właściwie możliwe jest to tylko w momencie rozpoznania całego incydentu i szczegółowego dochodzenia. Z takimi przypadkami w trakcie standardowych działań zespołu mamy do czynienia bardzo rzadko. Właściwie jedynym niebudzącym wątpliwości, co do przyczyn, przypadkiem jest spam, który jak to wcześniej zaznaczyliśmy został potraktowany oddzielnie.



Rysunek 9 - Przyczyna ataku

3.3.1.8 Spam

Jak to zostało wspomniane wcześniej w roku 2002 zarejestrowaliśmy 2518 przypadków spam'u. Reakcja na te przypadki oprócz trudnych prób wyeliminowania źródła spam'u mają również za zadanie ustalenie jak największej liczby źle skonfigurowanych serwerów pocztowych, które są wykorzystywane przez sapm'erów. W przypadku ustalenia takiego serwera kontaktujemy się z jego właścicielem i przekazujemy wskazówki dotyczące poprawy konfiguracji.

Znakomita większość przypadków spam'u sklasyfikowana jest w następujący sposób:

- atakującym jest *Zawodowy przestępca;*

- używa on zazwyczaj *skryptu lub programu;*

- wykorzystuje najczęściej dziurę w *konfiguracji;*

- spam wiąże się z odnotowywaniem nielegalnego, przepełniającego łącza i inne zasoby, ruch czyli *flood* ;

- jest to atak na *sieć sieci;*

- jego rezlutatem jest *kradzież zasobów;*

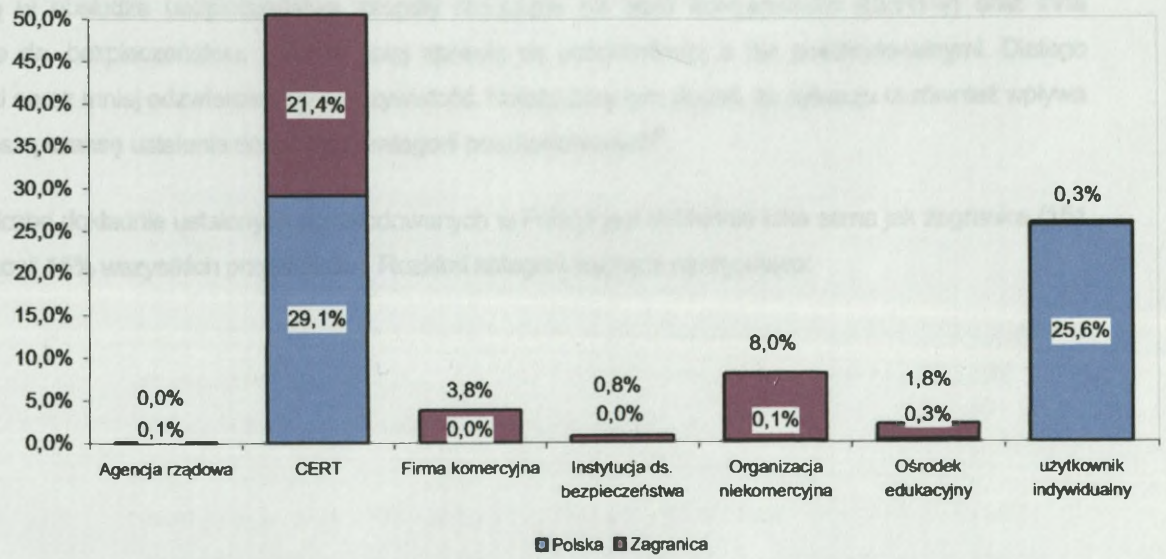
- a przyczyną zazwyczaj chęć uzyskania *korzyści finansowej*, znacznie rzadziej osiągnięcie korzyści politycznej.

3.4 Źródło zgłoszenia PNBT

Źródła zgłoszenia przypadków podzielono na 7 podstawowych kategorii[7]:

- Agencja rządowa;
- CERT;
- Firma komercyjna;
- Instytucja ds. bezpieczeństwa (inna niż CERT);
- Organizacja niekomercyjna;
- Ośrodek edukacyjny;
- Użytkownik indywidualny;

Każda z tych kategorii była podzielona na podmiot krajowy i zagraniczny. W ten sposób powstało 14 kategorii, które prezentowane są na poniższym wykresie.



[7] W stosunku do roku 2001 nastąpił zwiększenie liczby kategorii o 3. Dotychczasowe kategorie to: użytkownik indywidualny, CERT, instytucja ds. bezpieczeństwa, firma-organizacja.

Rysunek 10 - Źródła zgłaszania PNBT.

Z wykresu widać, że w tej kategorii prym wiodą instytucje typu CERT oraz użytkownicy indywidualni (głównie krajowi). Liczba zgłoszeń krajowych (55%) przewyższa liczbę zgłoszeń z zagranicy (37%).

3.5 Źródło ataku

W obsługiwanych przez nasz zespół przypadkach, w 94% udało się ustalić źródło ataku. Należy oczywiście wziąć pod uwagę, że wiele z tych adresów było tzw. adresami pośrednimi, które intruz wykorzystał w celu ukrycia rzeczywistego źródła ataku. Nie posiadamy informacji jak dużo było tego typu przypadków.

W wielu przypadkach szczegóły dotyczące źródła ataku, CERT Polska pozostawiał do ustalenia poinformowanej osobie lub komórce, odpowiedzialnej w danej organizacji za bezpieczeństwo lub administrację sieci.

Podstawowym, ustalonym dokładnie (kraj i kategoria) źródłem ataków[8] są zagraniczne firmy komercyjne oraz polskie ośrodki edukacyjne - odpowiednio 7 i 4 procent wszystkich ataków. Oczywiście chodzi tu o pojedynczych intruzów wykorzystujących do ataku sieci tych firm i jednostek edukacyjnych.

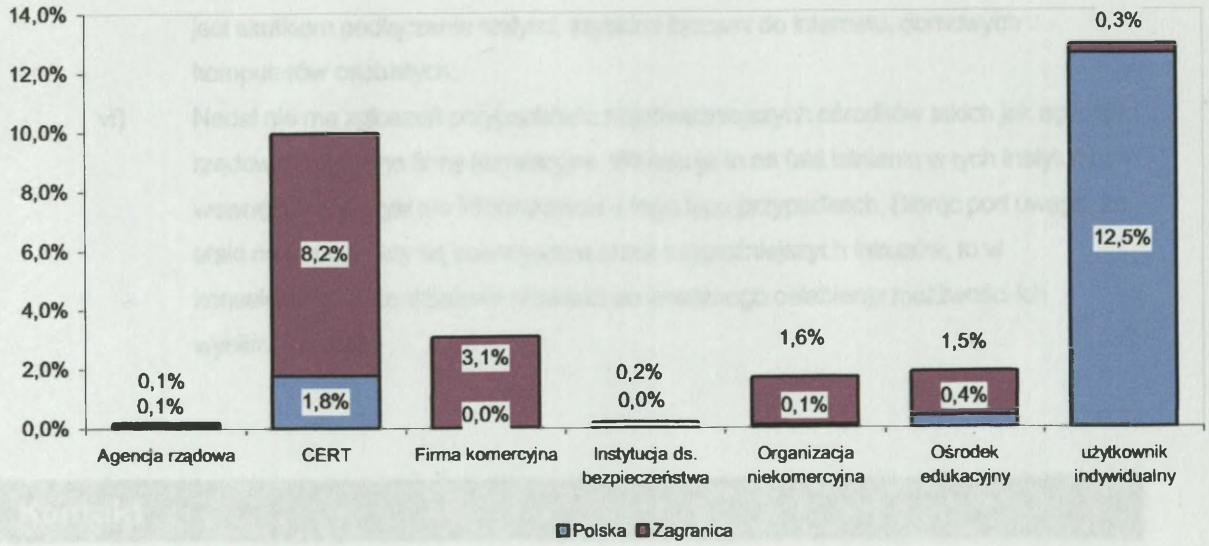
3.6 Poszkodowani

W tym roku po raz pierwszy wprowadziliśmy nową kategorię poszkodowanego. Do tej pory domyślnie poszkodowany wyszukiwany był wśród zgłaszających przypadki, jednak coraz większą rolę spełniają w obsłudze bezpieczeństwa zespoły reagujące na ataki komputerowe (CERT-y) oraz inne instytucje ds. bezpieczeństwa, które w całej sprawie są pośrednikami a nie poszkodowanymi. Dlatego statystyki coraz mniej odzwierciedlały rzeczywistość. Należy przy tym dodać, że sytuacja ta również wpływa na mniejszą szansę ustalenia dokładnych kategorii poszkodowanych[9].

Liczba dokładnie ustalonych poszkodowanych w Polsce jest dokładnie taka sama jak zagranicą (151 - co stanowi 15% wszystkich przypadków). Rozkład kategorii wygląda następująco:

[8] Ustalono to tylko w 12% przypadków

[9] Przy koordynacji PNBT pomiędzy CERT-ami przyjęte jest, że nie jest konieczna dokładna wiedza na temat poszkodowanego dla CERT-u którego zadaniem jest ustalenie sprawcy naruszenia bezpieczeństwa.



Rysunek 11 - Poszkodowani.

Warto zwrócić uwagę na stosunkowo duży procent CERT-ów wśród poszkodowanych. Głównym powodem znaczącej liczby tych zgłoszeń jest sam fakt istnienia wysokiego poziomu świadomości związanej z koniecznością zgłaszania przypadków, istniejącego wśród samych CERT-ów.

4 Wnioski i trendy

Poniżej zamieściliśmy głównie wnioski, jakie nasuwają się nam po analizie zebranych danych oraz wynikają z naszej codziennej pracy związanej z obsługą przypadków:

i) Polaryzacja wiedzy i świadomości dotyczącej zagrożeń teleinformatycznych. Rośnie zarówno procent posiadających dużą wiedzę i świadomość, jak i tych, którzy są bardzo słabo lub w ogóle nie zorientowani w tematyce bezpieczeństwa IT;

ii) Bezpieczeństwo w sieci zależy coraz bardziej od najsłabszego ogniwa, jakim staje się niski poziom dbania przez administratorów systemów o to, aby ich zasoby miały aktualne zabezpieczenia (tzw. łaty systemowe)

iii) Incydenty stają się coraz bardziej rozległe, coraz trudniej ustalić rzeczywistego atakującego i rzeczywistego poszkodowanego, który często nie jest bezpośrednio zaatakowany, ale w sposób istotny odczuwa skutki ataku na inne niż swoje zasoby;

iv) Coraz częściej to, co uważamy za źródło ataku, jest w rzeczywistości jedną z ofiar ataków. Źródła ataków w statystykach wskazują de facto na najgorzej zabezpieczone zasoby sieci;

v) Coraz więcej poszkodowanych jest wśród użytkowników indywidualnych, co zapewne jest skutkiem podłączenia stałymi, szybkimi łączami do internetu, domowych komputerów osobistych;

vi) Nadal nie ma zgłoszeń przypadków z najpoważniejszych ośrodków takich jak agencje rządowe i poważne firmy komercyjne. Wskazuje to na fakt istnienia w tych instytucjach wewnętrznej polityki nie informowania o tego typu przypadkach. Biorąc pod uwagę, że ataki na te podmioty są dokonywane przez najgroźniejszych intruzów, to w konsekwencji takie działanie prowadzi do znacznego osłabienia możliwości ich wyeliminowania.

5 Kontakt

Zgłaszanie incydentów:	cert@cert.pl, spam: spam@cert.pl
Informacja:	info@cert.pl
Strona WWW:	http://www.cert.pl/
Adres:	CERT POLSKA
	NASK
	ul. Wąwozowa18
	02-796 Warszawa
tel.:	+48 22 5231 274
fax:	+48 22 5231 399

Załącznik 4

CERT POLSKA

Raport 2001

Przypadki naruszające bezpieczeństwo teleinformatyczne

1 Wstęp

1.1 Informacje dotyczące zespołu CERT POLSKA

CERT(Computer Emergency Response Team) Polska jest zespołem powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w sieci Internet. CERT Polska działa od 1996 roku (do końca roku 2000 pod nazwą CERT NASK), a od roku 1997 jest członkiem FIRST (Forum of Incidents Response and Security Teams). Od roku 2000 członkiem europejskiej inicjatywy zrzeszającej zespoły reagujące – Trusted Introducer[1]. W ramach tych organizacji współpracuje z podobnymi zespołami na całym Świecie.

Do głównych zadań zespołu należy:

- rejestrowanie i obsługa zdarzeń naruszających bezpieczeństwo sieci
- alarmowanie użytkowników o wystąpieniu bezpośrednich dla nich zagrożeń
- współpraca z innymi zespołami IRT (Incidents Response Team) w ramach FIRST
- prowadzenie działań informacyjno edukacyjnych, zmierzających do wzrostu świadomości dotyczącej bezpieczeństwa teleinformatycznego (zamieszczanie aktualnych informacji na stronie www.cert.pl, organizacja cyklicznej konferencji SECURE)
- prowadzenie badań i przygotowanie raportów dotyczących bezpieczeństwa polskich zasobów Internetu
- niezależne testowanie produktów i rozwiązań z dziedziny bezpieczeństwa teleinformatycznego
- prace w dziedzinie tworzenia wzorców obsługi i rejestracji incydentów a także klasyfikacji i tworzenia statystyk

2 Statystyki CERT POLSKA

Zgodnie z powyższymi założeniami programowymi CERT POLSKA co roku przygotowuje i udostępnia statystyki dotyczące przypadków naruszenia bezpieczeństwa teleinformatycznego w polskich zasobach internetowych. Niniejszy raport jest szóstym z kolei raportem tego typu. Dotychczasowe (począwszy od roku 1996) raporty dostępne są na stronie CERT POLSKA (http://www.cert.pl/ -> Opracowania CERT Polska -> Raporty)

[1] 22 listopada 2001 zespół uzyskał najwyższy poziom zaufania Trusted Introducer Level 2.

3 Statystyka przypadków naruszających bezpieczeństwo teleinformatyczne[2]

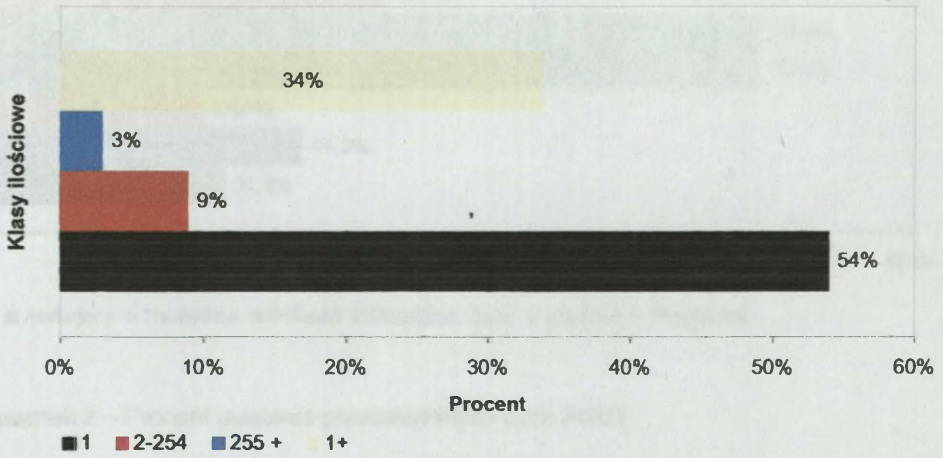
3.1 Liczba przypadków naruszających bezpieczeństwo teleinformatyczne

W roku 2001 odnotowano 741PNBT.

3.2 Liczba zaatakowanych komputerów

Wśród stwierdzonych PNBT odnotowaliśmy wiele takich, w trakcie których przeprowadzono atak na więcej niż jeden komputer czy inny obiekt sieciowy. W statystyce rodzajem „1+" określono te wszystkie przypadki kiedy wiadomo było, że liczba zaatakowanych komputerów była większa niż jeden, jednak nie było możliwe ustalenie konkretnej wartości.

Mimo tego w ponad 50% przypadków mieliśmy do czynienia z atakiem na jeden komputer.



Rysunek 1 - **Liczba zaatakowanych komputerów w trakcie jednego ataku**

3.3 Typy odnotowanych ataków

Począwszy od 2001 roku CERT Polska rozpoczął klasyfikację incydentów zgodnie z propozycją John'a D.Howard'a i Thomas'a A.Longstaff'a, znaną pod nazwą „Common Language"[3] .

Dodatkowo, aby dobrze scharakteryzować rozkład rodzajów ataków w kontekście najbardziej popularnych ataków, przygotowaliśmy skróconą statystykę najczęściej odnotowywanych ataków szczegółowych, takich jak chociażby najbardziej znane wirusy (3.3.2).

---

[2] W dalszej części raportu przypadki naruszenia bezpieczeństwa teleinformatycznego określane będą skrótem PNBT

[3] Wszystkich zainteresowanych szczegółami tej klasyfikacji odsyłamy do publikacji *Common Language (http://www.cert.org/research/taxonomy_988667.pdf)*

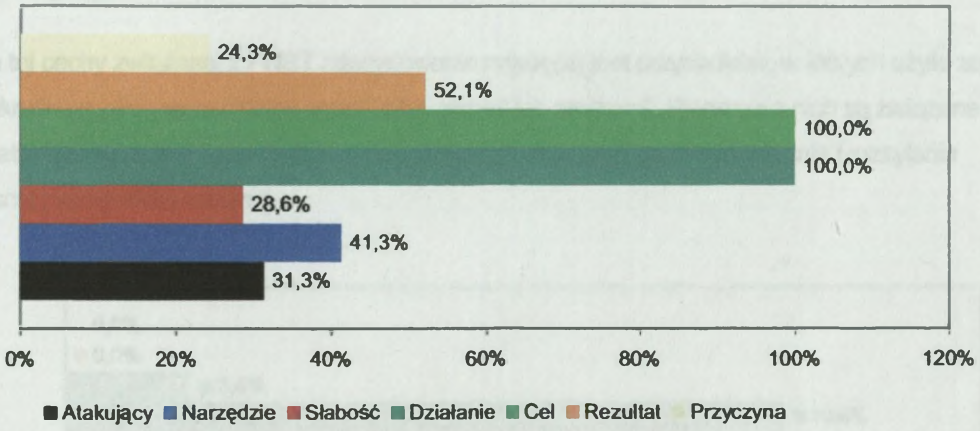
3.3.1 Klasyfikacja incydentów wg *Common Language*

Przypadki, w czasie obsługi których, można było zgromadzić dane pozwalające na wypełnienie wszystkich cech PNBT stanowią około 9%.

Należy zwrócić uwagę, że klasyfikacja *Common Language* z założenia jest klasyfikacją kompletną, dlatego zawiera również kategorie, które właściwie nie są zupełnie zgłaszane do zespołów reagujących podobnych do takiego jakim jest zespół CERT Polska (np.: ataki fizyczne). Niemniej jednak dla porządku i pełnego obrazu, w naszych statystykach nie pomijamy tych kategorii.

Poniższy wykres przedstawia w ilu przypadkach udało się ustalić daną cechę PNBT.

Najbardziej podstawową formą ataku komputerowego jest tzw. zdarzenie (*ang. event*). Cechami charakteryzującymi *zdarzenie* są *działanie (action)* jakie podjął intruz oraz *cel (target)* jaki zaatakował. W związku z tym wszystkie przypadki muszą i mają określone te dwie cechy.



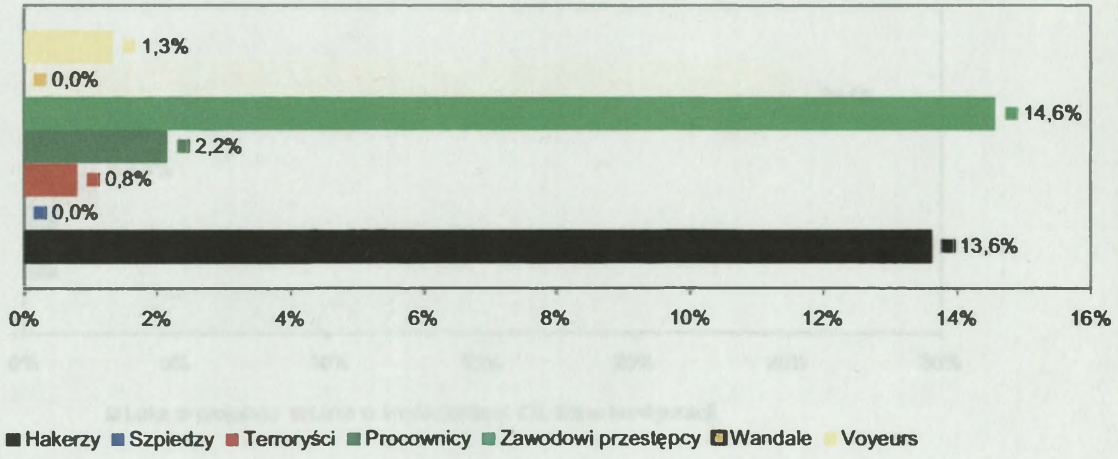
Rysunek 2 – Procent ustalenia poszczególnych cech PNBT.

Poniższe podpunkty pokazują rozkład procentowy w poszczególnych cechach opisujących PNBT

3.3.1.1 Atakujący[4]

Na poniższym wykresie widzimy rozkład procentowy związany z kategorią „atakujący". Dwie najważniejsze grupy to hakerzy i zawodowi przestępcy. Termin „zawodowy przestępca" należy traktować umownie. W rzeczywistości w tej kategorii znaleźli się wszyscy, którzy rozsyłają niezamawianą korespondencję.

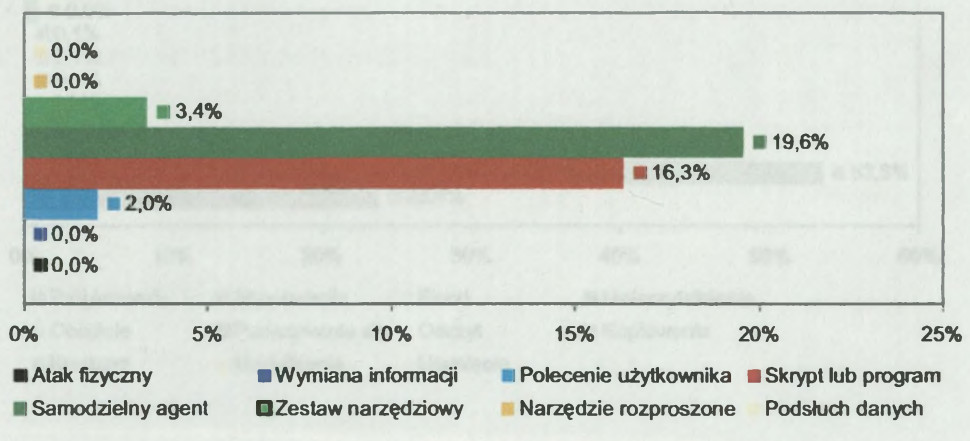
[4] W tej kategorii nie zostało przetłumaczone pojęcie *voyeurs*, ze względu na jego specyficzne znaczenie i brak jednoznacznego odpowiednika w języku polskim.
Voyeurs - *Atakujący, którzy atakują komputery dla podniecenia wywołanego uzyskaniem niejawnych informacji.*



Rysunek 3 - Klasyfikacja atakujących

3.3.1.2 Narzędzia

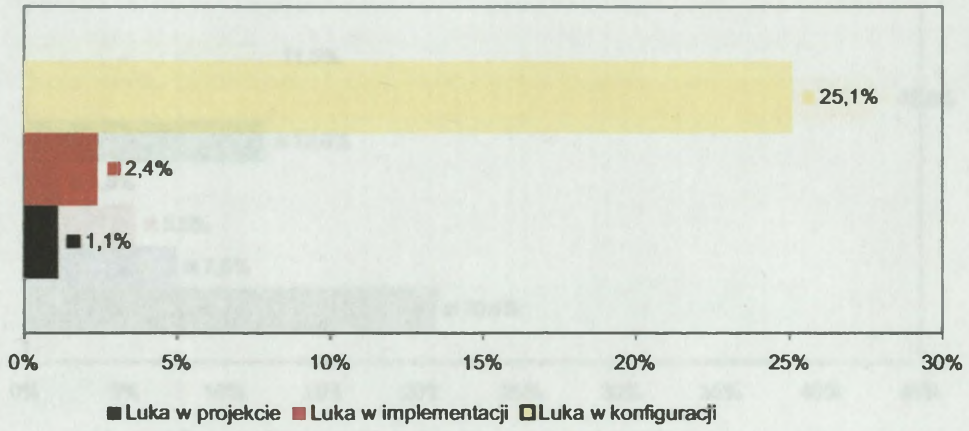
Dla tej cechy związanej z PNBT zdecydowanie najwięcej jest przypadków, w których użyte zostały narzędzia określane jako „samodzielny agent" albo „skrypt lub program". Pierwsze z nich są związane z masowymi atakami wirusów (Code Red, Nimda), zaś drugie z przypadkami skanowania i rozsyłania niezamawianej poczty elektronicznej.



Rysunek 4 - Klasyfikacja używanych narzędzi ataku

3.3.1.3 Atakowana słabość systemu

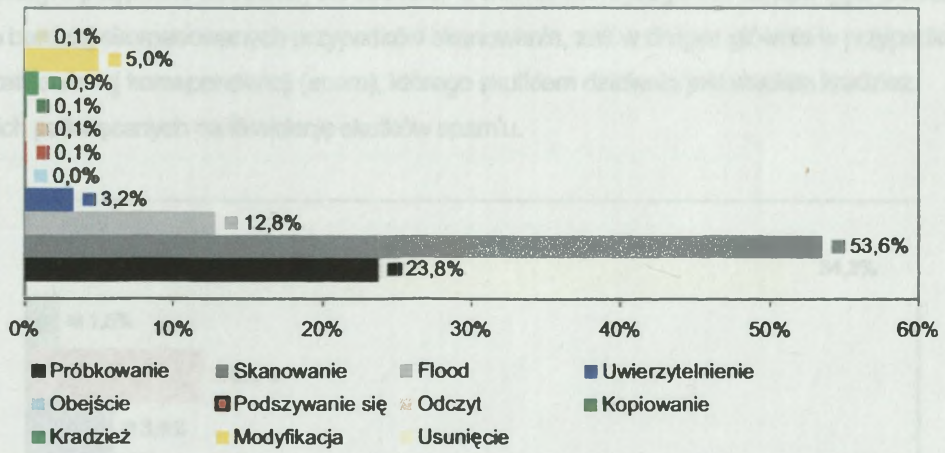
Luka w konfiguracji systemów komputerowych jest zdecydowanie najczęstszą przyczyną ataków komputerowych. Z doświadczeń CERT Polska wynika, że znacznie rzadszą przyczyną są luki w implementacji i zaprojektowaniu systemu. Zapewne przyczyną takiego a nie innego wyglądu tej statystyki jest stosowanie automatycznych narzędzi przez *script kiddies*, które to narzędzia (patrz również 5v) zazwyczaj są nastawiane na wykorzystanie luk w konfiguracji.



Rysunek 5 - Klasyfikacja wykorzystania poszczególnych luk w systemie

3.3.1.4 Nieautoryzowane działanie

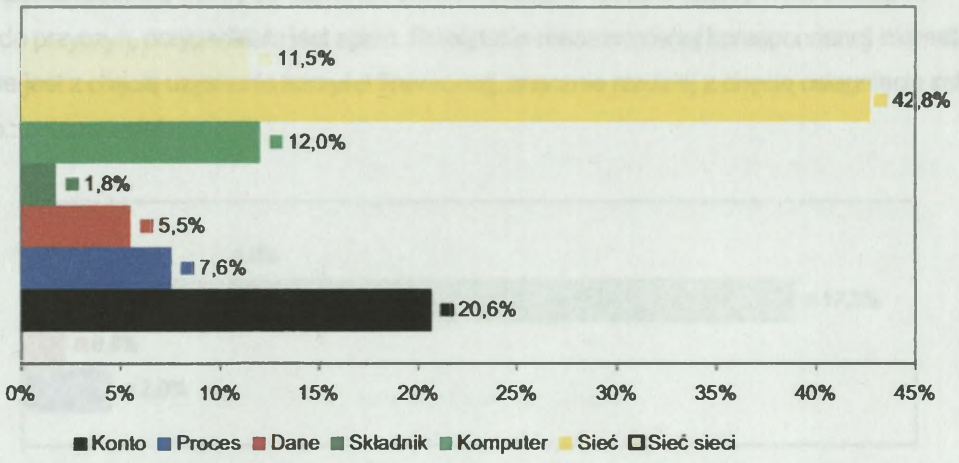
Zdecydowanie największy procent nieautoryzowanego działania stanowią przypadki próbkowania i skanowania. Wśród tych przypadków również znajdują się ataki powiązane z robakami internetowym (Code Red, Nimda). Odnotowane przypadki nieautoryzowanego *uwierzytelnienia i modyfikacji*, powiązane są zazwyczaj z przypadkami włamania, a czasami włamania połączonego z podmianą strony WWW.



Rysunek 6 - Nieautoryzowane działanie podejmowane przez atakującego

3.3.1.5 Cel ataku

Cel ataku jest drugą podstawową cecha opisującą PNBT. Najczęściej, wśród PNBT w roku 2001, celem ataku były całe sieci lub nawet sieci sieci (*internetworks*), co wynika z popularności przypadków skanowania. Naruszenie bezpieczeństwa *składnika* infrastruktury, jest w rzeczywistości atakiem fizycznym, tego typu ataki nie są zgłaszane do CERT Polska.

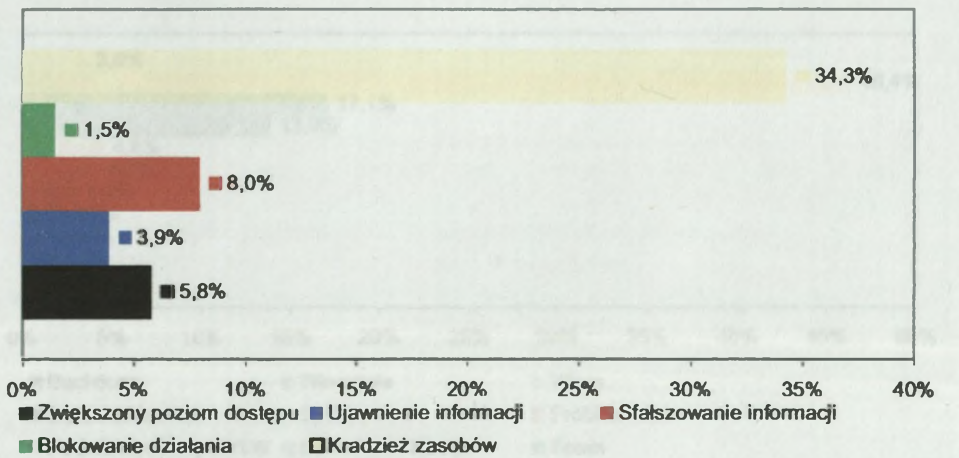


Rysunek 7 - Cel ataku

3.3.1.6 Rezultat

Wśród rozpoznanych skutków działania intruzów zdecydowanie na pierwszy plan wysuwa się *kradzież zasobów*. Dwa podstawowe przypadki wpływające na taki stan rzeczy to kradzież zasobów rozumianych jako moc obliczeniowa oraz rozumianych jak praca ludzka.

W pierwszym przypadku do nadużycia dochodzi w momencie wystąpienia ataków typu *Denial of Service* oraz co bardziej skomasowanych przypadków skanowania, zaś w drugim głównie w przypadku rozsyłania nie zamawianej korespondencji (*spam*), którego skutkiem działania jest swoista kradzież zasobów ludzkich poświęcanych na likwidację skutków spam'u.

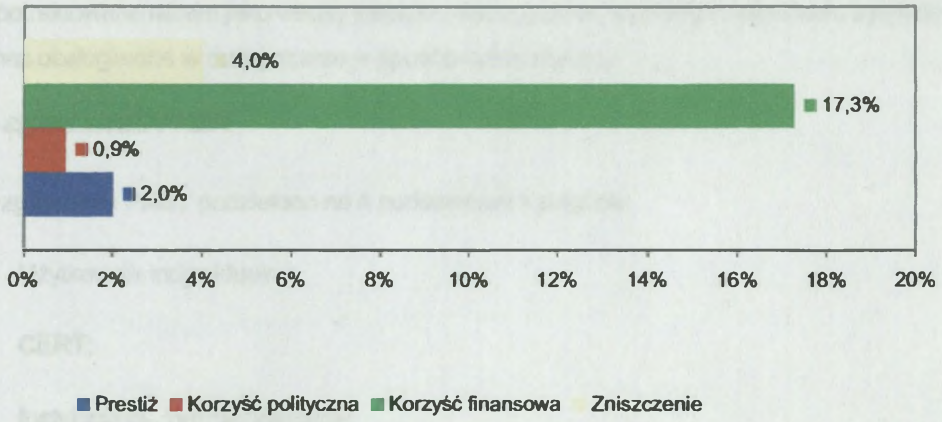


Rysunek 8 - Rezultat przeprowadzonego ataku

3.3.1.7 Przyczyna

Przyczynę, która decydowała o wystąpieniu PNBT jest bardzo trudno ustalić, dlatego procent odpowiedzi na pytanie *Co było przyczyną działalności intruza?* jest niewielki. Właściwie możliwe jest to tylko w momencie rozpoznania całego incydentu i szczegółowego dochodzenia. Z takimi przypadkami w trakcie

standardowych działań zespołu mamy do czynienia bardzo rzadko. Właściwie jedynym nie budzącym wątpliwości, co do przyczyn, przypadkiem jest spam. Rozsyłanie niezamawianej korespondencji niemalże w 100% powiązane jest z chęcią uzyskania korzyści finansowej, znacznie rzadziej z chęcią osiągnięcia celów politycznych (np.: propagandę)

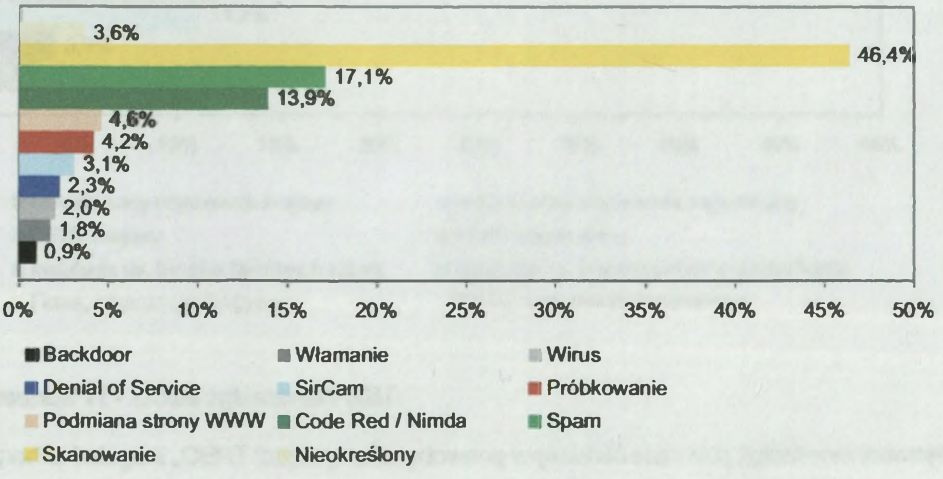


Rysunek 9 - Przyczyna ataku

3.3.2 Klasyfikacja wg charakterystycznych ataków

W celu uzupełnienia formalnej statystyki *Common Language* zamieszczamy również dodatkowe zestawienie, w którym można odnaleźć niektóre charakterystyczne kategorie, których nie ma w klasyfikacji *Common Language*

Poniższy wykres przedstawia charakterystyczne rodzaje ataków w roku 2001



Rysunek 10 - Charakterystyczne rodzaje ataków

Jak widać z powyższego wykresu obserwujemy wyraźną przewagę różnego rodzaju skanowania i próbkowania, które łącznie stanowiły ponad 50 % (50,6) obsługiwanych przypadków. Znaczącą rolę odgrywają również przypadki spam'u. Oczywiście przypadki, które są do nas zgłaszane wiążą się zazwyczaj

z dużą uciążliwością lub z tzw. open relay'em, czyli takim skonfigurowaniem serwera pocztowego, które pozwala na wykorzystywanie go przez spamer'ów do rozsyłania niezamawianej korespondencji.

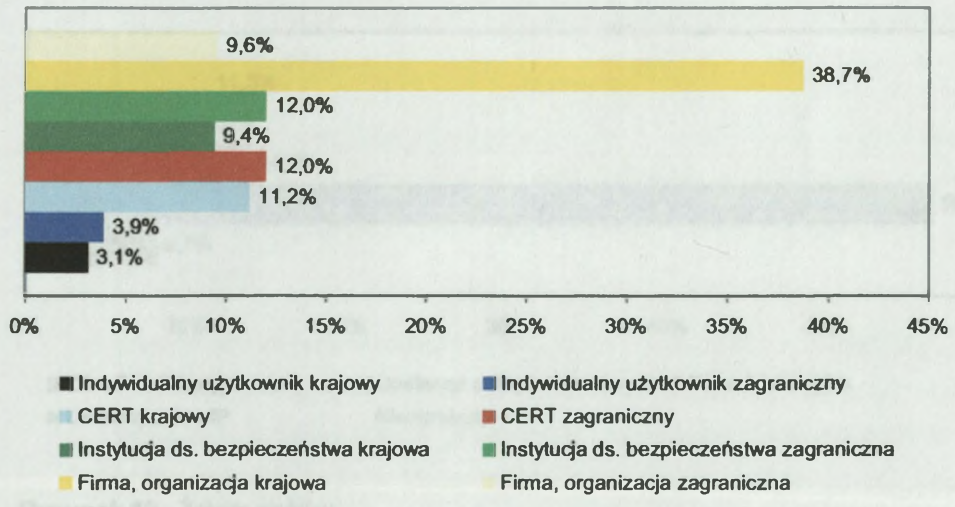
Trzecią pozycję (13,9%) na liście najbardziej popularnych rodzajów ataków zajmują łącznie potraktowane Code Red i Nimda, szczególnie aktywne w letnich miesiącach zeszłego roku. Code Red i Nimda zostały potraktowane razem jako wirusy sieciowe działające na podobnych zasadach, były one również przez nas obsługiwane w dużej mierze w sposób automatyczny.

3.4 Źródło zgłoszenia PNBT

Źródła zgłoszenia PNBT podzielono na 4 podstawowe kategorie:

- Użytkownik indywidualny;
- CERT;
- Instytucja ds. bezpieczeństwa;
- Firma, organizacja;

Każda z tych kategorii była podzielona na podmiot krajowy i zagraniczny. W ten sposób powstało 8 kategorii, które prezentowane są na poniższym wykresie.



Rysunek 11 - Źródła zgłaszania PNBT.

W przypadku kategorii „CERT krajowy" zdecydowaną większość stanowią zgłoszenia wewnętrzne CERT Polska związane ze spam'em i wirusami, które zostały przesyłane na adres poczty elektronicznej przeznaczony do zgłaszania incydentów. Zgodnie z powyższymi statystykami 62,5% zgłoszeń pochodziło z Polski, pozostałe z zagranicy.

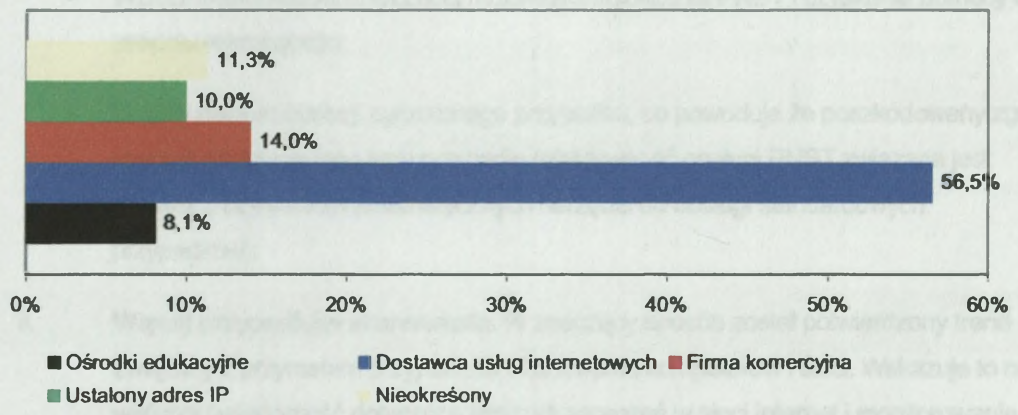
3.5 Źródło ataku

W obsługiwanych przez nasz zespół PNBT w blisko 90% udało się ustalić źródło ataku. Należy oczywiście wziąć pod uwagę, że wiele z tych adresów było tzw. adresami pośrednimi, które intruz wykorzystał w celu ukrycia rzeczywistego źródła ataku. Nie posiadamy informacji jak dużo było tego typu przypadków. W wielu przypadkach szczegóły dotyczące źródła ataku, CERT Polska pozostawiał do ustalenia poinformowanej osobie lub komórce, odpowiedzialnej w danej organizacji za bezpieczeństwo lub administrację sieci.

Kategorie na jakie podzieliliśmy źródła ataku są następujące:

- Ośrodki edukacyjne;
- Operatorzy telekomunikacyjni (ISP)[5];
- Firmy i organizacje;
- Ustalony Adres IP;

Jak widać wśród tych kategorii jest też pozycja „Ustalony adres IP". W tych przypadkach nie można było w prosty sposób zaklasyfikować źródła do innej kategorii dlatego zastosowano taką kategoryzację mówiącą o tym, że mimo braku dokładnych danych źródło ataku jest znane.



Rysunek 12 - Źródła ataków

Jak widać z powyższego wykresu podstawowe źródło ataków stanowią użytkownicy indywidualni, korzystający z połączeń oferowanych przez dostarczycieli usług internetowych.

[5] kategoria ta w dużej mierze dotyczy również użytkowników indywidualnych, którzy są klientami ISPs

4 Kooperacja przy obsłudze PNBT

W trakcie obsługi PNBT współpracowaliśmy z wieloma zespołami typu CERT z całego świata. Zdecydowana większość z nich jest członkami międzynarodowych organizacji FIRST (Forum of Incident Response and Security Teams) lub/i Terena TF-CSIRT (Task Forces Computer Security Incident Response Teams). O transgraniczności przestępstw komputerowych niech świadczy lista krajów, z których pochodziły zespoły reagujące współpracujące z nami przy wyjaśnianiu incydentów: Australia, Dania, Finlandia, Francja, Holandia, Korea Południowa, Meksyk, Niemcy, Rosja, Stany Zjednoczone, Szwajcaria, Wielka Brytania, Włochy.

W Polsce szczególną rolę odgrywała współpraca z zespołem TPSA Abuse Team, dodatkowo sporadycznie z zespołami bezpieczeństwa dostarczycieli usług internetowych.

5 Wnioski i trendy

i. **Wzrost PNBT.** Z roku na rok odnotowujemy coraz to większą liczbę PNBT. Mimo niepodważalnego trendu związanego z rzeczywistym przyrostem tego typu przypadków, należy zwrócić uwagę również na inne istotne czynniki, wpływające na ostateczne statystyki:

   - Wzrost świadomości dotyczącej możliwości zgłoszenia PNBT i uzyskania pomocy od zespołu reagującego;
   - Lepszy poziom obsługi zgłoszonego przypadku, co powoduje że poszkodowany zgłosi również następne tego typu przypadki (efektywność obsługi PNBT związana jest również z używaniem automatycznych narzędzi do obsługi standardowych przypadków);

ii. **Więcej przypadków skanowania.** W znaczący sposób został potwierdzony trend związany z przyrostem przypadków skanowania komputerów i sieci. Wskazuje to na większą świadomość dotyczącą istnienia zagrożeń w sieci Internet i monitorowanie tych zagrożeń oraz, jak należy przypuszczać, używanie w większym stopniu systemów detekcji zagrożeń (IDS), które pozwalają na zwiększoną wykrywalność i łatwiejszą dokumentację tych przypadków.

iii. **Po raz pierwszy *Common Language*.** W tym roku po raz pierwszy przedstawiliśmy statystyki oparte o klasyfikację *Common Language*. Wyniki tych statystyk pokazują jak trudno jest określić wszystkie dane dotyczące incydentu, okazuje się, że jest to możliwe tylko w przypadku bardzo szczegółowego rozpoznania przypadku. Najważniejszymi cechami tej klasyfikacji jest kompletność i jednoznaczność co w przyszłości pozwoli porównać statystyki z różnych lat. Dlatego też ta klasyfikacja będzie kontynuowana w latach następnych.

iv. **Automatyczne ataki.** Obserwowane przypadki skanowania i rozprzestrzeniania się wirusów sieciowych wskazują na fakt powszechnego wykorzystywania przez hakerów automatycznych narzędzi, zarówno w fazie ich przygotowywania (np.: tworzenie wirusów) jak i przeprowadzania (np.: skanowanie, włamania za pomocą tzw. rootkits, czy działanie robaków sieciowych). Zdecydowana większość tych przypadków związana jest działalnością tzw. *script kiddies*, którzy w swojej działalności wykorzystują gotowe narzędzia, nie znając w rzeczywistości sposobu ich działania.

v. **Słabość konfiguracji.** Działanie wspomnianych *script kiddies* powiązane jest zazwyczaj z wykorzystaniem znanych słabości, które nie zostały załatane przez administratorów. Potwierdzeniem tego faktu jest statystyka pokazująca, że największa liczba ataków związana była z wykorzystaniem luk w konfiguracji systemu. Dzięki temu jeszcze raz można się przekonać jak istotną rolę w zarządzaniu systemem informatycznym odgrywa sprawa odpowiedniego i systematycznego łatania istniejących w nim dziur.

vi. **Sprawcy ataków.** Jeśli chodzi o źródło ataków, to najpoważniejszym zagrożeniem dla bezpieczeństwa systemów komputerowych są klienci dostarczycieli usług internetowych. Najczęściej są to klienci działający na łączach dodzwanianych (*dial-up*). Niestety, wciąż istnieje błędne przekonanie o anonimowości tego typu połączenia, chociaż należy przyznać, że w przypadku działania z zagranicy, ustalenie sprawcy jest trudniejsze, co nie znaczy że niemożliwe. Przy wyjaśnianiu tych spraw dochodzą po prostu trudności organizacyjne polegające na wymianie odpowiednich danych pomiędzy CERT'em a administratorami ISP. Wymaga to dobrej woli i potwierdzenia wiarygodności obydwu stron. Znaczący odsetek PNBT, w których źródłem ataku jest adres ISP sprawia, że kwestia dobrej współpracy z ISPs odgrywa i odgrywać będzie bardzo ważną rolę.

6 Kontakt

Zgłaszanie incydentów:	cert@cert.pl
Informacja:	info@cert.pl
Web site:	http://www.cert.pl/
Adres:	CERT POLSKA
	NASK
	ul. Wąwozowa18
	02-796 Warszawa
tel.:	+48 22 5231 274
fax:	+48 22 5231 399

Załącznik 5

CERT POLSKA

Raport 2000

Przypadki naruszające bezpieczeństwo teleinformatyczne

1 Wstęp

1.1 Informacje dotyczące zespołu CERT POLSKA

CERT(Computer Emergency Response Team) Polska jest zespołem powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w sieci Internet. CERT Polska działa od 1996 roku (do końca roku 2000 pod nazwą CERT NASK), a od roku 1997 jest członkiem FIRST (Forum of Incidents Response and Security Teams). W ramach tej organizacji współpracuje z podobnymi zespołami na całym Świecie.

Do głównych zadań zespołu należy:

- rejestrowanie i obsługa zdarzeń naruszających bezpieczeństwo sieci
- alarmowanie użytkowników o wystąpieniu bezpośrednich dla nich zagrożeń
- współpraca z innymi zespołami IRT (Incidents Response Team) w ramach FIRST
- prowadzenie działań informacyjno edukacyjnych, zmierzających do wzrostu świadomości dotyczącej bezpieczeństwa teleinformatycznego (zamieszczanie aktualnych informacji na stronie www.cert.pl, organizacja cyklicznej konferencji SECURE)
- prowadzenie badań i przygotowanie raportów dotyczących bezpieczeństwa polskich zasobów Internetu
- niezależne testowanie produktów i rozwiązań z dziedziny bezpieczeństwa teleinformatycznego
  prace w dziedzinie tworzenia wzorców obsługi i rejestracji incydentów a także klasyfikacji i tworzenia statystyk

1.2 Statystyki CERT POLSKA

Zgodnie z powyższymi założeniami programowymi CERT POLSKA co roku przygotowuje i udostępnia statystyki dotyczące przypadków naruszenia bezpieczeństwa teleinformatycznego w polskich zasobach internetowych. Niniejszy raport jest piątym z kolei raportem tego typu. Dotychczasowe (począwszy od roku 1996) raporty dostępne są na stronie CERT POLSKA (http://www.cert.net.pl/statystyki.html)

2 Statystyka przypadków naruszających bezpieczeństwo teleinformatyczne[1]

Poniżej przedstawione zostały statystki dotyczące PNBT. W statystykach odrębnie potraktowano przypadki przesyłania (otrzymywania) nie zamawianej poczty elektronicznej, zwanej popularnie tzw. spamem. Decyzję taką podjęto ze względu na niewspółmiernie dużą liczbę tych przypadków w stosunku do przypadków pozostałych. Przypadki spamu zostały odnotowane oddzielnie, w rozdziale specjalnie temu poświęconym.

[1] W dalszej części raportu przypadki naruszenia bezpieczeństwa teleinformatycznego określane będą skrótem PNBT

2.1 Ilość przypadków naruszających bezpieczeństwo teleinformatyczne

W roku 2000 odnotowano 126 PNBT.

2.2 Ilość zaatakowanych komputerów

W 126 PNBT zaatakowano 292 komputery (hosty). Znacząca ich część – 206, co stanowi ponad 70% powiązana była z przypadkami włamania do systemu (182 przypadki) i próbami włamania do systemu (24 przypadki), czyli z najgroźniejszymi PNBT.

2.3 Typy odnotowanych ataków

Dokonano analizy rozkładu procentowego typów ataków zarówno w ujęciu ilości PNBT, jak też ilości zaatakowanych komputerów. Jak wynika z poniższych danych rozkłady te zasadniczo się różnią.

2.3.1 Typy odnotowanych ataków w ujęciu PNBT

Największy procent typów PNBT stanowiły próby włamania do systemów – 19% (24 przypadki). Następnie odnotowano taki sam udział procentowy włamań i skanowania hostów (15%, 19). Poniżej zestawienie wszystkich typów PNBT:

- Próba włamania do systemu – 19% (24)
- Włamanie do systemu – 15% (19)
- Skanowanie hosta – 15% (19)
- Skanowanie sieci – 13% (17)
- Ataki DoS (*ang. Denial of Service*) – 13% (16)
- Ataki na WWW serwer (podmiana strony) – 6% (8)
- Mail bombing – 5% (6)
- Skanowanie firewall – 3% (4)
- Inne (nielegalne oprogramowanie, social engeenering) – 10% (13)

Wszystkie przypadki skanowania (host, firewall, sieć) stanowią łącznie blisko 32% wszystkich PNBT i zdecydowanie jako łączna kategoria wysuwają się na czoło klasyfikacji.

2.3.2 Typy odnotowanych ataków w ujęciu zaatakowanych komputerów

W sytuacji rozważania rozkładu typów ataków w ujęciu zaatakowanych komputerów sytuacja zmienia się dosyć znacząco. Tu zdecydowanie na pierwszy plan wybijają się przypadki włamania – 62% (182). Łączny procent różnego rodzaju skanowania (firewall, host, sieć) wynosi 14% (40). Poniżej zestawienie wszystkich typów:

- Włamanie do systemu – 62% (182)
- Próby włamania – 8% (24)
- Ataki DoS (*ang. Denial of Service*) – 7% (19)
- Skanowanie hosta – 7% (19)

- Skanowanie sieci – 6% (17)
- Ataki na WWW serwer (podmiana strony) – 3% (8)
- Mail bombing – 2% (6)
- Skanowanie firewall – 1% (4)
- Inne (nielegalne oprogramowanie, social engeenering) – 4% (13)

2.3.3 Spam

Zdecydowanie największą ilość PNBT stanowiły przypadki spamu, dlatego z pewnych względów (wyjaśnienie powyżej na początku rozdziału) zostały one potraktowane oddzielnie.

Odnotowywane przypadki spamu wiązały się z pewnością z używaniem narzędzi automatycznych do generacji spamu. Przypadki jakie zostały zgłoszone do CERT POLSKA pochodziły głównie z sieci da.uu.net.

W ciągu roku do CERT POLSKA zgłoszono ponad 1 200 przypadków spamu.

2.4 Źródła odnotowanych ataków

Głównym źródłem odnotowanych ataków były sieci nadzorowane przez ośrodki edukacyjne, takie jak wyższe uczelnie, szkoły (głównie szkoły średnie) oraz instytuty naukowe. Łącznie wszystkie te ośrodki stanowiły 42% (53) źródeł odnotowanych PNBT.

Źródłem 29% (36) PNBT był intruz korzystający z zasobów dostarczyciela usługi internetowej (*ang. Internet Service Provider*), z czego około 9% powiązanych było z adersami IP ogólnie dostępnej sieci publicznej.

15% (19) PNBT powiązanych było z kontem firmowym jako źródłem ataku.

Najmniej znaczący procent - 7% (9) stanowiły źródła inne.

Również 7% (9) stanowiły przypadki, w których nie ustalono źródła ataku.

2.5 Źródła zgłoszenia incydentów

W przypadku źródła zgłoszenia incydentu wyróżniano 3 kategorie: CERT lub inna instytucja ds. bezpieczeństwa, użytkownik krajowy, użytkownik zagraniczny. W tej materii procent przypadków rozkłada się mniej więcej równo i wygląda następująco:

- Użytkownik krajowy – 35% (45)
- Użytkownik zagraniczny – 33% (41)
- CERT lub inna instytucja ds. bezpieczeństwa – 32% (40)

3 Wnioski

Biorąc pod uwagę niewielki procent zgłaszania incydentów (różne źródła podają wielkości rzędu kilku procent) szacowana liczba zgłoszonych incydentów a tym samym ilości incydentów w polskich zasobach Internetu nie jest mała. Nadal niestety jednak odnotowuje się dużą niechęć do zgłaszaniu incydentów. Powody są różne, ale z pewnością w największej mierze

decydują te, które dotyczą obawy przed utratą wizerunku firmy jako firmy bezpiecznej co na mocnym, konkurencyjnym rynku jest zadaniem niezwykle ważnym.

Z dużym prawdopodobieństwem, można zaryzykować stwierdzenie że odnotowany niewielki procent przypadków związanych z atakami blokującymi serwisy nie do końca odpowiada rzeczywistości. Ubiegły rok na całym świecie stał pod znakiem skomasowanych ataków DDoS i DoS, które dotknęły nie jedną, także te największe, firmę. Być może ataki tego typu stały się na tyle powszechne, że przestano je zgłaszać traktując jako normalną część związaną z obsługą urządzeń sieciowych dołączonych do Internetu. Jednak należy zastrzec, że są to tylko przypuszczenia i CERT Polska nie posiada szczegółowych danych na ten temat.

W trakcie obsługi zgłaszanych incydentów dosyć wyraźnie zarysował się fakt nie posiadania przez pokrzywdzonych odpowiednich procedur, które pozwalają na usystematyzowane działanie w przypadku wystąpienia zagrożenia. Często wynikiem braku tych procedur jest chaotyczne działanie, które w pierwszej kolejności przekłada się na reinstalację zaatakowanego systemu, co oczywiście jest skuteczne z punktu widzenia działania serwisu (choć czasami niestety nie na długo), ale uniemożliwia skuteczne pozyskanie informacji zmierzających do ustalenia sprawcy przestępstwa komputerowego.

Choć niewątpliwe stan świadomości dotyczącej bezpieczeństwa teleinformatycznego jak i sam poziom tego bezpieczeństwa poprawił się w ciągu kilku ostatnich lat to nadal napotykamy na przypadki elementarnych błędów związanych z wdrożeniem i obsługą systemów informatycznych.

4 Trendy

CERT Polska prowadzi swoje statystyki od 1996 roku. Począwszy od tego czasu liczba odnotowywanych incydentów stale rośnie.

W swoich obserwacjach odnotowaliśmy coraz więcej zgłaszanych incydentów, które nie kończą się sukcesem intruza ale naruszają w pewien sposób bezpieczeństwo zaatakowanych systemów, chociażby poprzez obciążenie osób odpowiedzialnych za ich bezpieczeństwo dodatkowymi obowiązkami kontroli i audytu zaatakowanego systemu. Świadczy to niewątpliwie o wzroście świadomości wśród polskich internautów. Coraz mniej jest tych którzy nie potrafią odpowiedzieć jednoznacznie na pytanie czy ich sieć była atakowana czy też nie.

Typy odnotowywanych ataków w drastyczny sposób się nie zmieniają na przestrzeni lat. Od lat najbardziej popularne są ataki na system poczty elektronicznej, ataki polegające na skanowaniu poszczególnych komputerów czy też całych sieci, ataki na serwery WWW, ataki zmierzające do blokady serwisu. Pewne ataki całkowicie lub częściowo zniknęły z naszej mapy typologicznej. Rzadziej odnotowujemy ataki bezpośrednio na konta użytkowników czy też na serwery *news*. Częściej występują bezpośrednie ataki na aplikacje i procesy. Na początku działalności naszej organizacji ataki te były znacznie bardziej popularne. Popularność tę w dniu dzisiejszym przejęły głównie ataki związane ze skanowaniem.

Od lat stałym elementem rejestrowanego zestawu typologicznego jest również spam, który szczególnie w zeszłym roku przyjął gigantyczne rozmiary.

5 Tabela zbiorcza

Typy odnotowanych ataków

Typ	*Ujęcie – PNBT*		*Ujęcie – host*	
	Procent	*Ilość*	*Procent*	*Ilość*

Włamanie do systemu	15	19	62	182
Próba włamania do systemu	19	24	8	24
Skanowanie sieci	13	17	6	17
Skanowanie host'a	15	19	7	19
Skanowanie firewall'a	3	4	1	4
Ataki DoS	13	16	7	19
Ataki na WWW	6	8	3	8
Mail bombing	5	6	2	6
Inne	10	13	4	13
Ogółem	**100**	**126**	**100**	**292**

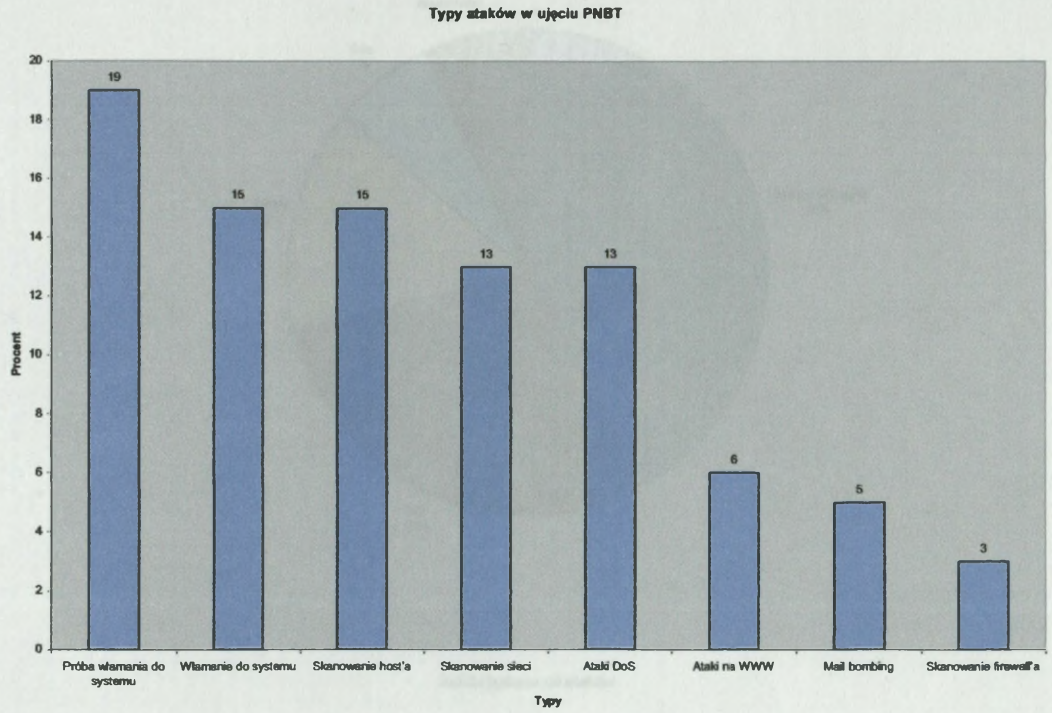
Źródła odnotowanych ataków

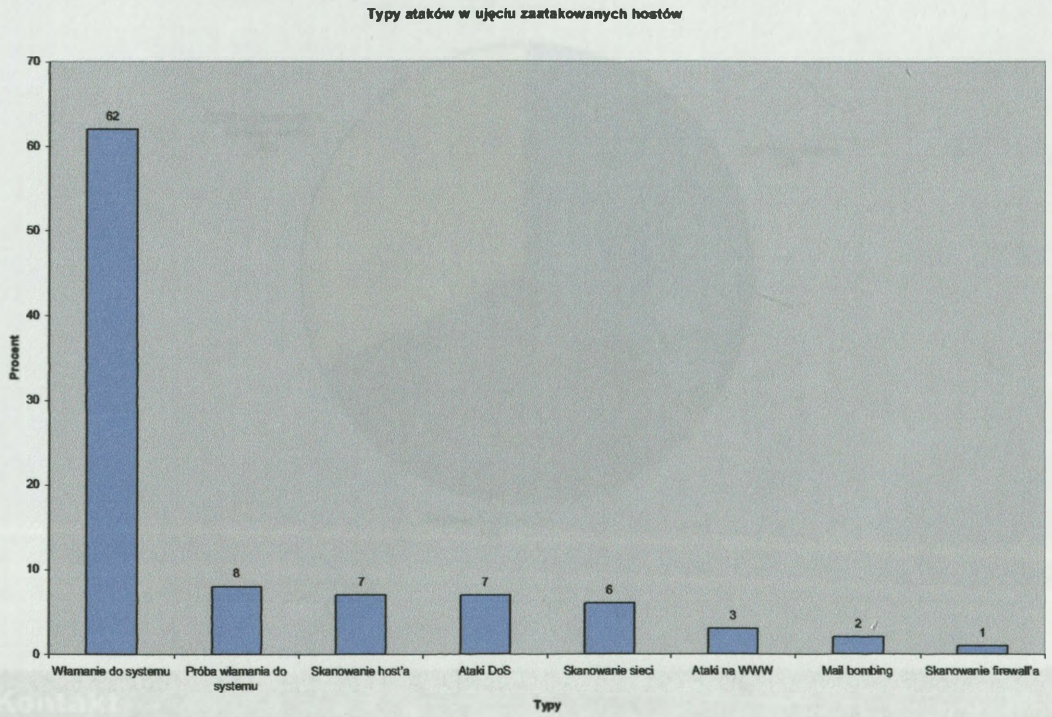
Źródło	*Procent*	*Typ*
Ośrodki edukacyjne	42	53
ISP	29	36
Firma	15	19
Inne	7	9
Nieustalone	7	9
Ogółem	**100**	**126**

Źródła zgłoszenia incydentów

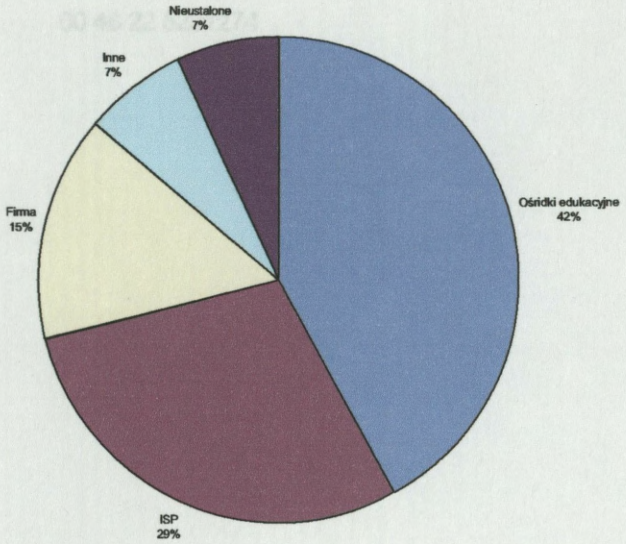
Źródło	*Procent*	*Typ*
Użytkownik krajowy	35	45
Użytkownik zagraniczny	33	41
CERT lub instytucja ds. Bezpieczeństwa	32	40
Ogółem	**100**	**126**

6 Wykresy

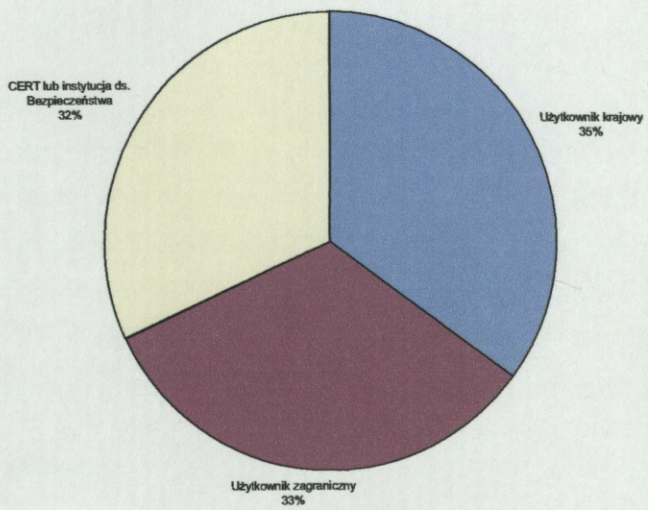

Typy ataków w ujęciu PNBT
Procent
Typy
19
15
15
13
13
6
5
3
Próba włamania do systemu
Włamanie do systemu
Skanowanie host'a
Skanowanie sieci
Ataki DoS
Ataki na WWW
Mail bombing
Skanowanie firewall'a


Typy ataków w ujęciu zaatakowanych hostów
Procent
Typy
62
8
7
7
6
3
2
1
Włamanie do systemu
Próba włamania do systemu
Skanowanie host'a
Ataki DoS
Skanowanie sieci
Ataki na WWW
Mail bombing
Skanowanie firewall'a

Źródła ataków



Źródła zgłoszenia ataków



7 Kontakt

e-mail: cert@cert.pl

Web site: http://www.cert.pl/

Adres: CERT POLSKA

ul. Bartycka 18

00-716 Warszawa

tel./fax: 00 48 22 5231274

W stosunku do roku 1998 CERT NASK w roku 1999 odnotował wzrost liczby zarejestrowanych incydentów naruszających bezpieczeństwo. Nie był to jednak tak duży wzrost jak w latach poprzednich. W roku 1999 liczba zarejestrowanych incydentów niewiele przekroczyła 100. Trzeba podkreślić, że rejestrowane są tylko oficjalne zgłoszenia (najczęściej pocztą elektroniczną), które dotyczą rzeczywistych przypadków związanych z naruszeniem bezpieczeństwa lub rażącym naruszeniem netykiety.

Typologia ataków

Wśród ataków największy procent dotyczy ataków wykorzystujących rozmaite metody skanowania poszczególnych komputerów w sieci Internet (hostów) a także skanowania całych podsieci. Łatwy dostęp do oprogramowania służącego do skanowania, często reklamowanego pod hasłem ,,sprawdź bezpieczeństwo swojego komputera" niewątpliwie poważnie przyczyniło się do popularności tego typu ataku. Wciąż popularne są też ataki na serwer z wykorzystaniem oprogramowania typu common gateway interface (CGI) wskazujących na chęć przejęcia istotnych informacji przez intruza z serwera WWW. Prawie 10% przypada w roku 1999 na ataki typu blokowanie usługi (DoS - Denial of Service) a światowe wydarzenia z początku roku 2000 potwierdzają coraz

większe zainteresowanie intruzów taką formą ataków. CERT NASK odnotowuje także przypadki tzw. uciążliwego spamu to jest spamu, wielokrotnym źródłem którego są ci sami użytkownicy, lub którego zakres negatywnego oddziaływania jest duży. Takich przypadków CERT NASK odnotował ponad 12 % z całej liczby incydentów. Z uwagi na wzrost ilości pojawiającego się w Internecie spamu CERT NASK nie jest jednak w stanie obsługiwać wszystkich przypadków związanych z tym zjawiskiem. Co warte podkreślenia spośród zarejestrowanych w 1999 roku incydentów 11% stanowiły typowe przypadki włamań.

Źródła ataków

Wśród prawdopodobnych źródeł ataków podobnie jak przed rokiem poważny procent zajmują adresy z umownie określanej sfery akademicko-naukowej. Nie jest to już jednak jak w poprzednich latach grupa dominująca. W roku 1999 największy procent ataków pochodził z kont w firmach komercyjnych. Drugą dużą grupę źródeł ataków stanowiły konta i dostawców internetu oraz publiczny dostęp do sieci poprzez TP S.A.

Efekt ataków

Podobnie jak rok wcześniej wśród zarejestrowanych ataków więcej jest tych, które wg zgłaszających zostały skutecznie odparte, niż tych które skończyły się przejęciem przez intruza praw administratora systemu. Potwierdza to fakt, że tylko nieliczne incydenty zgłaszane są do oficjalnych statystyk, i rzadko, kto chce się przyznawać do tego, że jego sieć została skutecznie zaatakowana. Jest to zjawisko ogólnoświatowe. Niestety największy procent odnosi się do sytuacji, w której poszkodowany nie jest w stanie ustalić poniesionych strat i często nie ma na to już szans gdyż system jest niezwłocznie reinstalowany.

Cel ataku i źródło zgłoszenia

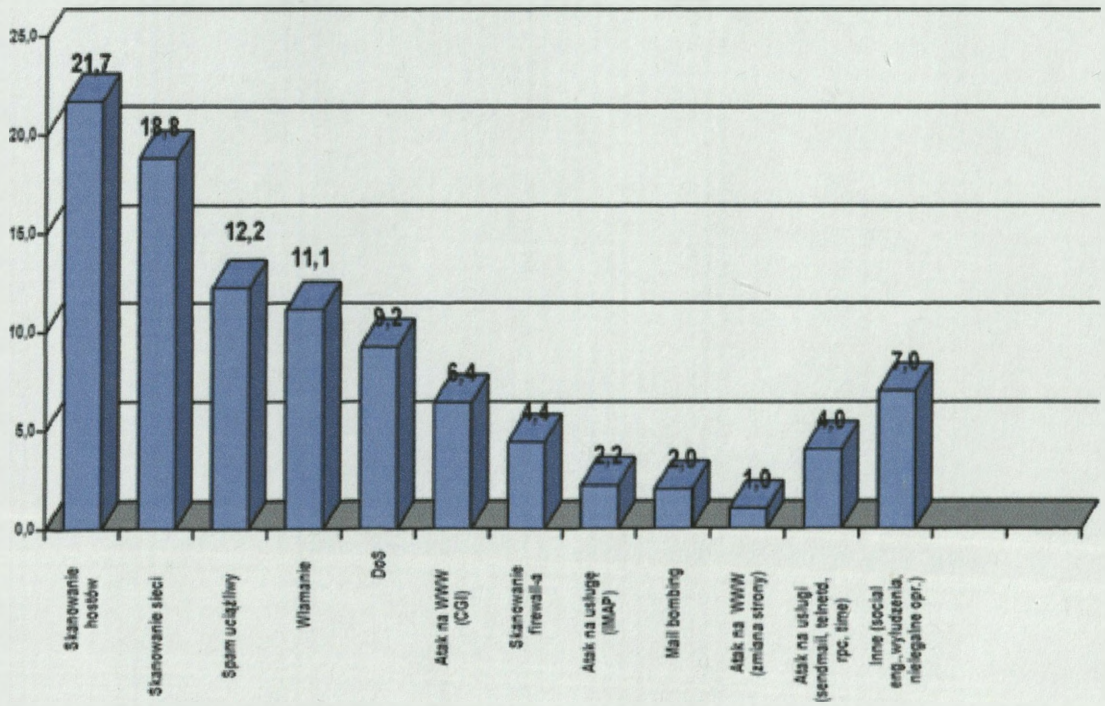
Większość, blisko 75%, zgłaszanych do CERT NASK incydentów pochodzi od użytkowników sieci - z czego około połowa to użytkownicy polscy a połowa to użytkownicy zagraniczni. Pozostałe 25% zgłoszeń pochodzi od instytucji, które w swojej działalności zajmują się walką z nadużyciami w sieci czyli innych zespołów reagujących (IRT) lub Policji, ze zdecydowanym wskazaniem na te pierwsze. Wśród poszkodowanych - podobnie ja w roku 1998 - dokładnie 50 % jest użytkowników zagranicznych i 50 % użytkowników polskiej sieci Internet. Wśród użytkowników polskich procentowo największą grupę docelową ataków stanowią jednostki naukowe bądź akademickie (20%) oraz firmy prywatne (ok.12%). Pokaźny procent ataków dotyczy także operatorów i dostawców usług telekomunikacyjnych. W roku 1999 zaobserwowano także utrzymywanie się trendu powstawania w ramach struktur firmowych zespołów lub osób odpowiedzialnych za sprawy bezpieczeństwa teleinformatycznego. CERT NASK częstokroć pełni rolę koordynacyjną w wymianie informacji między zainteresowanymi użytkownikami i zespołami bezpieczeństwa, ze szczególnym uwzględnieniem spraw międzynarodowych.

Problemy z typologią i klasyfikacją

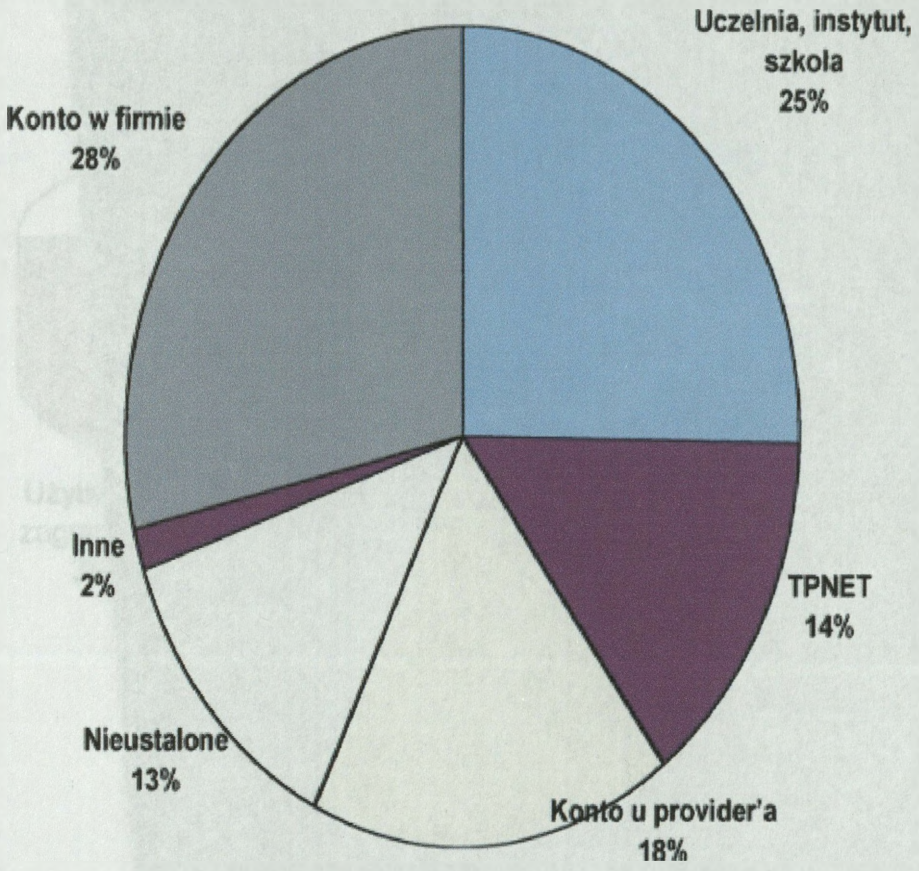
Przygotowując rokrocznie statystyki rejestrowanych incydentów CERT NASK napotyka na problem braku spójnej klasyfikacji i typologii ataków, którą można by się posłużyć w celu sklasyfikowania i zaprezentowania danych w taki sposób aby w możliwie standardowy sposób operować pojęciami związanymi z typami ataków. Niestety na świecie nie istnieje wspólny, obowiązujący wszystkich język pojęciowy w zakresie zdarzeń naruszających bezpieczeństwo sieci. Pewne próby stworzenia jednoznacznych klasyfikacji zostały podjęte w USA oraz w dwóch krajach europejskich - daleko jest jednak do stworzenia jakiegoś standardu. W ubiegłym roku CERT NASK podjął lokalnie pracę nad stworzeniem zrębów nowoczesnej klasyfikacji. Zespół chętnie udostępni wyniki swych prac w tym zakresie wszystkim zainteresowanym.

Poniżej przedstawiono kilka diagramów ilustrujących dane statystyczne zebrane w ramach pracy CERT NASK w roku 1999.

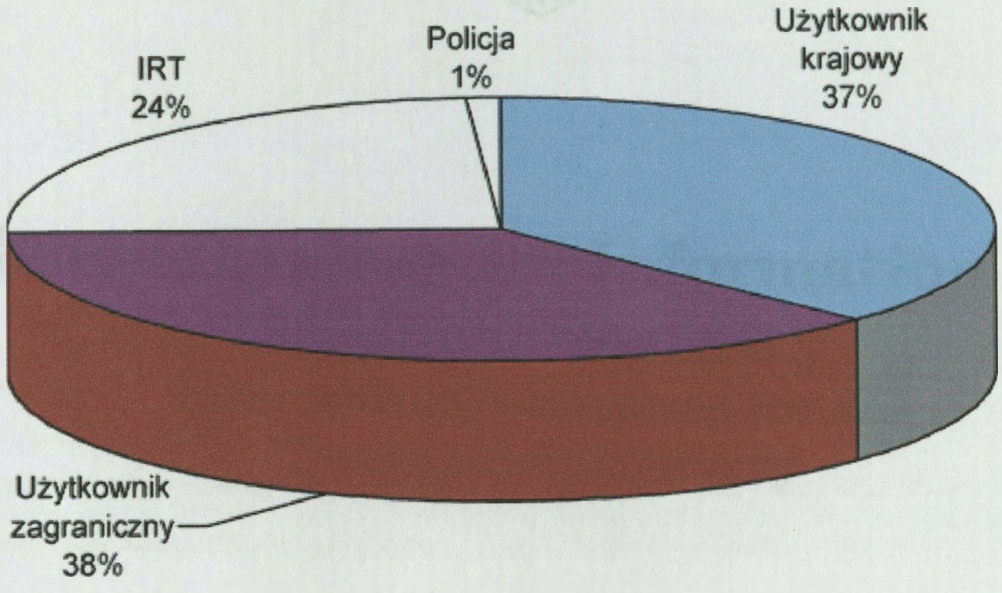
Wykres nr1. Procentowy rozkład typów ataków, 1999.



Wykres nr 2. Procentowy rozkład źródła ataków,1999.



Wykres nr 3. Procentowy rozkład źródła zgłoszenia ataków, 1999.



Grand Strategy for Information Age National Security

Information Assurance for the Twenty-first Century

Lt Col Kevin J. Kennedy, USAF
Col Bruce M. Lawlor, USARNG
Capt Arne J. Nelson, USN

Air University Press
Maxwell Air Force Base, Alabama

August 1997

Disclaimer

Opinions, conclusions, and recommendations expressed or implied within are solely those of the author(s) and do not necessarily represent the views of Air University, the United States Air Force, the Department of Defense, or any other US government agency. Cleared for public release: distribution unlimited.

Contents

Illustrations

About the Authors

The authors were National Security Fellows at Harvard University, Kennedy School of Government, during the 1995–96 academic year, when they researched and wrote this paper.

Col (sel) Kevin J. Kennedy, USAF, is a command pilot, whose most recently completed assignment was as deputy operations group commander at Whiteman Air Force Base. His previous flying assignments include duty as an operations officer of a B-52 bombardment squadron, chief of Wing Safety in the B-52/KC-135 training wing, chief of training in a B-52 squadron and as a T-37 instructor pilot. He has over 3,200 flight hours. His staff assignments include chief, Joint Strategic Planning Staff Briefing Branch, B-1B/B-52 strategic employment planner at Strategic Air Command Headquarters, and as an Air Staff training officer at the Pentagon. Colonel Kennedy is currently commander of the 608th Air Operations Group at Barksdale Air Force Base, Louisiana. He is a graduate of the United States Air Force Academy and holds master's degrees in national security and strategic studies from the Naval War College and human relations from Central Michigan University.

Col Bruce M. Lawlor, USARNG, is a National Guard officer who has commanded the 86th Armor Brigade and the 1-172 Armor Battalion, Vermont Army National Guard. He has served as an executive officer, staff officer, and commander at all levels in an armor brigade. He holds a BS in political science and juris doctor from the George Washington University. Colonel Lawlor is currently pursuing an MA in national security studies from Norwich University. He is a practicing attorney with national board certification in civil litigation and holds advocate status from the National College of Advocacy.

Capt Arne J. Nelson, USN, a naval aviator, commanded Helicopter Combat Support Squadron Four, homeported in Italy, during Operations Desert Shield and Storm, Provide Comfort in Northern Iraq, and Sharp Edge in Liberia. With over 3,500 flight hours, 3,200 in H-53 helicopters, his extensive operational experience involved flying tours in helicopter combat support and helicopter mine countermeasures squadrons, and included fleet replacement squadron instructor duty. A qualified joint staff officer, he served as executive assistant to the USACOM Director for Operations. Captain Nelson is currently the head of the Joint Operations and Plans Branch in the Chief of Naval Operations at the Pentagon. He is a graduate of the University of New Mexico and the Armed Forces Staff College, and holds an MS from the University of Southern California and an MA from the Naval War College.

Introduction

The Information Age brings enormous benefit to the United States; however, US dependence upon technology results in a new strategic threat aimed at the information systems that control key aspects of our military, economic, and political power.

New Strategic Threat

Overwhelming US conventional military might suggests that future competitors may embrace grand strategies that avoid directly attacking US defense forces and focus on undermining our national will to fight by exploiting our reliance upon information systems, present technological vulnerability, and the democratic method of governing. This threat would be most effective in situations where US force application is discretionary and the desirability of its employment is not clear-cut. Though it will never equate to the strategic threat of physical occupation by conventional military forces, it is a potent coercive policy weapon.

We believe the current US grand strategy for national security is obsolete because:

1. It is based upon industrial age threats and defenses that have limited information age applicability.
2. It fails to defend against structured information attacks threatening US centers of gravity.
3. It is still reliant upon DOD as sole provider of national defense.

New Information Age Realities

Six information age realities produce a significant change to the national security environment.

Information technologies have created a fifth dimension of conflict. Recognizing the uniqueness of this dimension highlights the limited relevance of the world's most powerful army, navy, and air force in defending strategic centers of strength from information attacks. The sum of its conventional forces is far more potent than any would challenge conventionally, but is an inadequate deterrent to deflect information weapons or protect information targets.

In this new dimension, *the rapid exploitation of information can produce significant advantages in warfare and in commercial competition.* Leaders who exploit information technology may seize the initiative, get inside an opponent's decision-making cycle, and thereby limit or channel the options available to it.

Moreover, in the Information Age, interconnectivity and dispersed computing power have greatly expanded access to and dependence upon information, making the places it resides (databases, communication networks, logic programs) more susceptible and

attractive targets. Therefore, *information itself must be protected.* Information can be used as a weapon to corrupt or destroy, or it can be the target of an attack.

For as long as defensive countermeasures lag behind innovative use of offensive information weapons, the US will have *new strategic vulnerabilities that make traditional notions of US physical sanctuary less meaningful.* Heavy US dependence upon information systems, combined with today's worldwide interconnectivity of computer systems, that have limited self-protection features, has created an avenue for attack of strategic assets. Financial institutions, public switch networks, power plants, and other strategic centers of strength could be at risk from information attacks, and military conventional forces can do very little to protect them.

Additionally, since the cost of entering information warfare is much less than that of conventional warfare, *traditional nation-states may not be the only potential attackers.*

If the US is to effectively build and execute a new grand strategy for national security, efforts beyond military defense must be employed and *new strategic measures of effectiveness are needed to prioritize both these efforts in both the offensive and defensive categories.*

Priorities for Protection within US Strategic Centers of Gravity

Our strategic framework divides US strategic centers of gravity into five categories: leaders, system essentials, infrastructure, population, and defense mechanism. Though the US defense establishment is able to defend these centers of gravity against physical attack, it cannot protect them against the flow of hostile information from outside sources. Future conflicts may see the use of both conventional and information weapons against these centers.

These weapons may be divided into categories according to their functions: conventional *physical destruction* weapons that target the enemy's physical assets for destruction; *corruption* information weapons that control, compromise, corrupt, or disable the operating software of targeted information networks and systems; and *perception management* information weapons that affect what an enemy's information systems portray as reality.

Juxtaposing these weapons functions with national centers of gravity produces a strategic framework, displays the information dimension of conflict, demonstrates the potential strategic effects of weapons employment, and conceptualizes both offensive and defensive campaigns. It also highlights shortfalls in present national security policies by suggesting the breadth of future battlefields, the accessibility of US centers of gravity, and the limitations of protecting against the employment of information weapons. In addition, it provides a reference for decision makers who must set priorities regarding which information systems require protection as strategic national security assets. Finally, it demonstrates how the scope of strategic warfare expands beyond the traditional dimensions of the battlefield into the broader information dimension of conflict.

While assertions of a national disaster may be somewhat premature, open source anecdotal evidence suggests the US is already vulnerable to information attacks. The

National Communications System labeled the threat to the US public switch network system as a "serious concern" in 1993 and said it was worse in their 1996 update, noting "threats [are] outpacing our deterrents while vulnerabilities are outpacing the implementation of protection measures."[1]

Moreover, applying the framework to a recent RAND war game shows that the enemy could make a concerted effort to attack the information systems that control the US system essentials to produce secondary impacts upon the US population, and thereby create pressures on US leaders to alter their chosen course. The analysis underscores the ramifications of information conflict for the nation's leaders and shows that perception management is the common thread in information conflicts. The degree of skill demonstrated in handling these issues determines the ability of government leadership to maintain the fragile link between itself and the people. Unless leaders can answer the people's questions satisfactorily, the danger exists that public pressure will force national security policy changes that may not be in the nation's best interest.

Other Complications: Authority, Responsibility, and Plurality

The threat to US information systems from corruption weapons is a clear and present danger that demands immediate attention. The pervasiveness of information technologies across the political, economic, military, and social fabric of American life poses a difficult defense solution that is far beyond DOD authority and responsibility. In the pluralistic US society, firmly founded upon the concepts of division of authority and separation of powers, authority will most likely never be given to any one government agency. Pluralism offers tremendous advantages over single party executive agents to ensure a healthy public debate. A pluralistic approach will more likely produce a public consensus that balances the need for government security and personal protection with US constitutional guarantees and American notions of individual liberty.

Conclusions

We need a new national security grand strategy that includes defending the nation's information infrastructure with the objective to develop the capability to detect, deflect, and defeat a structured information attack on the United States. Our strategic framework suggests *information assurance should be the theme for US defensive grand strategy.* The protection of the information and information systems that are critical to US strategic centers of gravity must become the catalyst for cooperation between government and civilian entities and the driving force behind the development of new national security policies. Information assurance provides the basis for a unified response to meet the strategic information threat.

Priority must be given to protecting information and information hardware that control the systems categorized as those system essentials that offer the most lucrative information targets. In addition, within the strategic centers associated with government, that is, leaders and the defense mechanism, the systems that permit command and

control and employment of military forces must also be protected. We believe the balance of information and information systems should be left to the private and commercial sectors.

Recommendation: A Strategic Plan for National Security

Vision: Information Assurance for the twenty-first century.

A national commitment that secures confidentiality, integrity, and availability of information and the reliability of information systems. A national consensus balancing government security and personal protection with US constitutional guarantees and American notions of individual liberties.

Mission: Identify and assess vulnerable information nodes within priority areas for protection.

- Identify and assess the strategic threat to US information and information systems.
- Develop proactive prevention and control measures that detect, deflect, and defeat intrusions into, or structured information attacks upon, priority areas for protection.
- Develop the capability to execute those plans.
- Develop national institutions that build US government and private sector equities in information assurance.

Goals: National Imperatives

- Lead a vigorous public debate to disclose that the Information Age presents security risks that are economic and political, and not solely military in nature.
- Unify a government/private sector response to protect the confidentiality, integrity, availability, and reliability of US information and information systems against the strategic information threat.
- Ensure that information assurance priority for protection is given to the specific system essentials strategic centers of gravity. Abandon the idea of universal protection in favor of selective defense of government and private sector information and information systems deemed critical to national security.
- Establish a National Information Assurance Council (NIAC) to make national security policy recommendations to the president, aimed at bringing about our national security vision of information assurance.
- Establish an Information Assurance Center (IAC), patterned after the Center for Disease Control and answerable to NIAC to perform surveillance, research,

prevention and control, and infrastructure functions within the information assurance mission.

- Expand US National Security Emergency Response Preparedness (NSERP) planning to include physical protection for key network switching and control systems that manage areas within our strategic centers of gravity designated for priority protection.
- Encourage the president and Congress to support the National Security Telecommunications Advisory Comittee's (NSTAC) effort to establish a Security Center of Excellence and expand the NSTAC concept by creating similar committees in areas designated for priority protection.

Goals: DOD Imperatives

- Secretary of Defense submits information assurance and its Information Age strategic implications as part of the next National Security Strategy and directs the chairman of the Joint Chiefs of Staff (CJCS) to promulgate a new national military strategy that addresses the information assurance vision and its wartime subset of information dominance.
- Retitle the Assistant Secretary of Defense (ASD) for Command, Control, Communications and Intelligence (C3I) as the ASD for information and incorporate continental United States (CONUS) defense against information attacks.
- Recommend a change to the Unified Command Plan. Designate CONUS as an area of responsibility (AOR) and task the commander in chief, Strategic Command (CINCSTRATCOM) or commander in chief, United States Atlantic Command (CINCUSACOM) with a CONUS-defensive information warfare responsibility. Assume aggressive, quantitative modeling and simulation effort for defensive information warfare.
- Assemble a DOD organization for defense information assurance. Use core competencies already available within DOD to replicate the health taxonomy used for national information assurance.
- Direct CINCUSACOM to restructure the Key Asset Protection Program (KAPP) by: (1) assessing key asset vulnerabilities to corruption information weapons as well as physical destruction weapons; (2) adding system essential priority areas for protection to the Key Asset List; (3) expanding the KAPP evaluation and review board to incorporate experts from appropriate fields; (4) expanding planning and training to incorporate new Key Asset List physical protection requirements; and (5) thoroughly documenting all actions needed to address information vulnerabilities.
- Merge KAPP analysis with current vulnerability net assessments to identify the potential repercussions of a structured information attack upon system essential assets. Assume aggressive, quantitative modeling and simulation effort for defensive information warfare. Recommend higher levels of information assurance for national security.

- Direct CINCUSACOM to review operational plans for the land defense of CONUS to incorporate potential impacts resulting from information attacks and degradations to the information infrastructure.

Notes

1. United States, National Communications System, *An Assessment of the Risk to the Security of Public Networks* (Washington, D.C.: National Communications System, December1995), ES-1.

Chapter 1

Grand Strategy Is More Than Military Strategy

The dawn of the Information Age suggests a reexamination of US defensive grand strategy.* This paper examines that issue, focusing on national security, not as the exclusive province of the Defense Department, but as the sum of political, economic, and military elements of national power and as the product of US national will.[1] Its purpose is to highlight the tenuous nature of current US national security policy, introduce information-age realities pertinent to future policy development, propose a framework for conceptualizing defensive grand strategy, and recommend both a vision and strategic plan to enact it. The paper intentionally avoids service-specific, operational, tactical, or technical discussions.

The US Should Reexamine Its Defensive Grand Strategy in the Information Age

Overwhelming US conventional military might suggests future competitors are likely to embrace grand strategies that avoid attacking US defense forces directly and instead focus on undermining its national will to fight by exploiting its reliance upon information systems, present technological vulnerability, and democratic method of governing. This information-strategic threat would be most effective in situations where US force application is discretionary and the desirability of its employment is not clear-cut. It will never equate to a strategic threat of physical occupation by conventional military forces, but it is a potent coercive policy weapon.

Information Technology Changes the Focus of Grand Strategy from the Military to Other National Power Centers

Carl von Clausewitz reasoned that commitment to war emerges from the confluence of three centers of national power: the people, the military, and the government.[2]

---

* **A Definition of Grand Strategy.** Grand strategy is the art and science of developing and using the political and economic powers of a nation, together with its armed forces, during peace and war, to further national interests, priorities, and policies. Grand strategy harnesses the elements of power for the entire nation and not just its military forces. Military strategy is a subset of grand strategy and is the art and science of employing the armed forces of a nation to secure grand strategy objectives by the application of force, or the threat of force. It does not define grand strategy but rather is defined by it. Thinking about grand strategy requires a different approach to conflict. It dictates a process of from-the-top-down analysis, moving from the general to the specific. All strategists must first conceptualize the conflict as a whole, that is visualize the battlefield at the strategic level. Only then can consistent operational and tactical discussions begin.

When these three centers of national power unify around a common purpose to be achieved by force of arms, an "interactive trinity" emerges that produces the national will to fight.

Clausewitz believed the most effective grand strategy to disrupt this "interactive trinity" and thereby gain victory was to defeat the enemy's military forces. He reasoned that such a defeat uncovered the enemy's other more vulnerable power centers and required it either to yield or face destruction of its leadership and people.[3] This precept has dominated much of western military thinking about grand strategy since Clausewitz's treatise, *On War,* was first published in 1832.

Today's information realm is a new and separate dimension of warfare that provides other nation-states and nonstate actors with direct access to US strategic centers of gravity and thereby generates a new and different national security environment. The nation's defense forces remain a viable deterrent to conventional military attack against the US population and its civilian political, economic, and social infrastructures. However, at present, they are neither structured nor empowered to defend against national-level information attacks, or information attacks outside of the DOD infrastructure, and therefore their ability to provide protection for these national power centers is problematic.[4] This development creates new strategic opportunities for the world's next generation of aggressors and significant problems for those who will be charged with defending against them.

Against this backdrop, three factors must be considered. First, the United States has become the world's most "wired" country. It depends upon complex, interconnected information network control systems for such necessities as oil and gas pipelines, electric power grids, national transportation systems, banking and financial transactions, commercial exchanges, and a host of other perhaps less essential activities.[5] This interconnectivity provides enormous economic, societal, and political advantages to the United States. However, it also makes these information control systems vulnerable to information weapons and therefore potentially inviting targets for US competitors.

Second, the defenses needed to protect the United States against information attacks are incomplete, making the world's most technologically advanced nation at the same time its most technologically vulnerable. Once adapted to military uses and coupled with organizational and doctrinal changes, information technology could significantly alter the battlefield equation.[6] Because of its advanced technology, the United States is poised to achieve such a breakthrough. However, capitalization on information technology elsewhere could provide strategic leverage to nations presently thought incapable of opposing the United States and enable them to emerge quickly from their military obscurity with significant, perhaps decisive, advantages in future conflicts. This will remain a possibility until such time as the United States has developed and fully implemented defensive countermeasures to information warfare. At present, defensive countermeasures are lagging behind available offensive systems.

Finally, the same technology that provides access to the American infrastructure also provides a variety of individual and group actors with unprecedented levels of direct contact with the US population and with US government officials. Such access promotes a healthy democracy. In the highly interconnected United States, public sentiment drives politicians to act, or to refrain from acting, as never before. Decision

makers must deal with the media in shaping public opinion that sets the limits beyond which US policy must not go. Information technology now provides others, both hostile and friendly, with the means to affect directly how Americans perceive their government's policies, societal norms, and needs for self-protection.*

There Is a Lack of Consensus Concerning the Threat

Arguments against this scenario center on three key issues: economic interdependence, infrastructure robustness, and the lack of technical expertise on the part of potential adversaries to carry out a structured information attack. These issues, when coupled with the requirement for an adversary to have solid intelligence for target selection, lead many to dispute the immediacy or validity of the threat on the US infrastructure.[7]

Those who doubt the nation is at risk claim that to conduct a structured information attack** on the US is virtually impossible, and that anything less (i.e., a focused, regional, or tactical attack) would not yield success. Economic interdependence, they claim, discourages information warfare because the costs of attacking US targets, for example, financial centers, outweighs any benefits gained. While nation-states may accept this premise, terrorists and other nonstate actors will care little for economic interdependence, and the ability to initiate information attacks while remaining anonymous diminishes the effectiveness of retaliation as a deterrent. The assertion that potential competitors lack technical expertise is belied by the record. Significant intrusions are happening today and in some cases are state-sponsored (see appendix A). The vulnerabilities discussed within this paper are all based on capabilities demonstrated by actual incidents. The assumption made is that malevolent actors will eventually capitalize upon demonstrated capabilities and known vulnerabilities to mount a structured attack.

Notes

1. Col Arthur F. Lykke Jr., lecture, US Army War College, Carlisle Barracks, Pa., July 1995.
2. Edward J. Villacres and Christopher Bassford, "Reclaiming the Clausewitzian Trinity," *Parameters* 25, no. 3 (Autumn 1995): 9–20.
3. Carl von Clausewitz, *On War,* ed. and trans. Michael Howard and Peter Paret (Princeton, N.J.: Princeton University Press, 1976), 90.

---

* The impact upon the US population of potential occupation by a foreign force has always weighed heavily upon US decision makers. Washington understood the vulnerability of the US population to British information warfare and both Grant and Lee were attuned to the vulnerability of their respective populations. The difference is that information technology provides competitors with the ability to impact the US population without occupation.

** According to Julie Ryan of Booz Allen, a strategic attack would be one that embodies an intention by an adversary to inflict overwhelming damage with a desired goal of 60 to 100 percent loss of capability over time. It requires the ability to purposefully target entities while coordinating time and location of attacks and inflicting certain specific levels of damage, and requires significant intelligence capability to include comprehensive understanding of target functionalities and processes the reliance placed on individual targets and cascading effects. It requires the ability to deliver the means of attack. The scale of the attack would be difficult to conduct covertly.

4. According to the Defense Science Board, there is no nationally coordinated capability to counter or detect a structured information attack, a problem that is made more difficult by the fact that many systems are not controlled by the Department of Defense (DOD). The Computer Security Act of 1987 limits DOD's ability to use its core expertise (e.g., National Security Agency) to help protect these systems and restricts it to protecting federal government systems that handle classified information. The act also assigns the National Institute of Standards and Technology (NIST) responsibility for protecting federal unclassified but sensitive information. No one is responsible for protecting commercial, public, and private systems upon which national viability depends. Department of Defense, *Information Architecture for the Battlefield* (Washington, D.C.: Defense Science Board, 1994), 36.

5. Michael Brown, an analyst with Science Applications International Corporation, postulates a hierarchy of information needs in which societies first use information, then come to rely upon it, and ultimately come to depend upon it. Once dependence occurs, the society begins to organize itself around information. He argues that in the case of the United States, such dependence creates vulnerabilities. Michael Brown, "Information Warfare and the Revolution in Military Affairs," *Seminar on Intelligence, Command and Control* (Cambridge, Mass.: Center for Information Policy Research, Harvard, 1995), 6.

6. Andrew W. Marshall, memorandum for the record, subject: RMA Update, 2 May 1994.

7. Martin C. Libicki, *What is Information Warfare?* (Washington, D.C.: Institute for National Strategic Studies, National Defense University, August 1995).

Chapter 2

The Nature of the Threat

In information war, if an enemy's information or information systems are threatened to the point where national leadership must take action, then information warfare is underway.

—John Alger
National Defense University

The Purpose of Warfare Is to Overcome an Enemy's Will to Resist

Clausewitz believed that war is "an act of violence to compel our opponent to fulfill our will."[1] The objective of grand strategy, in his model, is to achieve that purpose by disrupting the enemy's "interactive trinity" through defeat of its military component.[2] This is the paradigm that drives most grand strategy planning. There are other potential models, however, in which grand strategy may be able to achieve its objective without disarming an opponent. The experience of the United States in Vietnam is an example of strategic defeat in the absence of corresponding military defeat. The US departure from Somalia is an illustration of strategic withdrawal in a situation short of war where the US possessed overwhelming military superiority. Both of these instances suggest that actions generating internal political pressures within the United States can produce strategic consequences. For political systems, such as that of the United States, information warfare has the potential to generate enormous pressures on leaders to alter national policies. Accordingly, US grand strategists must view information attacks on this country not in the context of their immediate damage but in terms of their impact on the body politic.[3] In this regard, they represent yet another means of trying to compel an opponent to fulfill one's will.

Information Provides an Alternative Means of Attacking the National Will

The objective of information attacks would be to gain strategic leverage over US decision makers by generating political pressures within the US population to change national policies. Such attacks could provide a means by which adversaries could coerce US leaders to pursue policies more aligned with their adversaries' ends and objectives and without using conventional military force.

The efficacy of information as a weapon against the United States is predicated upon three factors: (1) vulnerable networked systems can be disrupted to launch a structured information attack, (2) malevolent actors will seek to take advantage of these vulnerabilities, and (3) the US population is able to generate political pressures that change national policy.

Anecdotal Evidence of Disrupted Networked Systems

Emerging anecdotal evidence continues to demonstrate the vulnerabilities of networked systems to significant disruptions through accidental or intentional input problems. For example, in 1991 there was a near total shutdown of telephone service in the Baltimore-Washington area as the result of a three-bit coding error where a "d" was replaced by a "6" in one byte of a software upgrade. This simple error caused disruption of AT&T long distance service to millions of customers for over four hours.[4]

In another incident, on 17 September 1991, AT&T announced that a power interruption had caused two public switches to fail. This failure forced the shutdown of major airports that rely on ground-based telephone lines for air traffic control communications in the New York, Boston, and Washington air route traffic control centers. The result was disruption of the civil aviation industry in these centers for days. The disruption in turn caused flight delays across the nation.[5]

In addition to system failures and software glitches, there is anecdotal evidence concerning malicious interference with information systems. A November 1988 virus (Morris worm), placed on the Internet by a college student, infected 6,000 host computers in less than two hours and cost between $100,000 and $10 million to clean up, affecting network links between Massachusetts Institute of Technology (MIT), University of California, Sandia Labs, Lawrence Livermore Labs, Los Alamos National Research Laboratories, and others.[6] In another incident, a Christmas card message sent over BitNet, a global academic network, landed in 2,800 machines in five minutes, including IBM's internal network. It took only five hours for the benign virus to spread 500,000 infections worldwide, forcing IBM to take the network down for several hours to accomplish repairs.[7]

In the military arena, anecdotal evidence suggests the United States has already become a target for information attacks by groups intent on frustrating US national defense policies. Shortly after Iraq's invasion of Kuwait in 1990, various groups and actors launched a worldwide effort to penetrate various sensitive US government and military computers. Both Washington and North Atlantic Treaty Organization (NATO) were targets. Dutch crackers penetrated host computers at Lawrence Livermore Laboratories, then branched out to access other systems across the United States. They successfully penetrated US military computer systems at least 34 times between April 1990 and May 1991. Pentagon officials report these same individuals offered to disrupt the US military's deployment to the Middle East in return for payment from Saddam Hussein in the amount of $1 million. Saddam spurned the offer (see appendix A for additional examples of information attacks).[8]

The anecdotal evidence suggests both nation-state and nonstate actors are already using the techniques of information conflict to launch limited, uncoordinated information

attacks against the United States. These attacks are a growing concern within the US government. In a report released in October 1994, the DOD's Defense Science Board (DSB) found that

> the nation is under IW [information warfare] attack today by a spectrum of adversaries ranging from the teenage hacker to sophisticated, wide-ranging illegal entries into telecommunications networks and computer systems. This threat arises from terrorist-groups or nation-states, and is far more subtle and difficult to counter than the more unstructured and growing problem caused by hackers. A large structured attack with strategic intent against the US could be prepared and exercised under the guise of unstructured hacker activities . . . [such a strike] could cripple operational readiness and military effectiveness [by delaying troop deployments and misrouting cargo planes, trains, and ships].[9]

Information attacks may be divided into structured and unstructured threats (fig. 2-1). Unstructured threats, sometimes referred to as Class 1 and 2 attacks, are aimed at individuals and corporations. Structured threats (Class 3 attacks) are aimed at nation-states or societies, are more analogous to traditional warfare, and are the information equivalent of a major regional conflict or total war. There have been no reported instances of Class 3 attacks to date. Together these attacks include a range of information activities from malicious and potentially dangerous computer pranks, to criminal hacking activities, to terrorist acts of destruction, through malevolently shaping a nation's perceptions and opinions, to executing intensely lethal attacks employing advanced information-based weapons during interstate conflict.[10]

Warfare is changing in the face of these threats and is adapting to them. We are witnessing the beginning of a new epoch in warfare that will supplement, and at times supplant, lethal combat on the battlefield, and at its core lies information warfare.[11] Just as the airplane's adaptation to military uses led to fights to establish air superiority, the emergence of information as a strategic weapon will likewise lead to conflicts in which the first order of battle will be to establish information dominance over the enemy. Future conflicts may or may not be as lethal as those in the past; however, they are likely to witness mass upheavals in civilian populations. Increasingly frequent reports of computer crime and the potential of info-terrorism have heightened awareness of the nation's information vulnerability as opposed to vulnerability of physical assets.[12] As Winn Schwartau observed,

> The victims are not only the targeted computers, companies, or economies, but the tens of millions of people who depend upon those information systems for their very survival. Take the power of class 1 and class 2 Information Warfare, multiply it tenfold, and you will begin to get a sense of the kind of damage that can be done. Class 3 Information Warfare creates chaos.[13]

The point of all this is not to suggest chaos on the information highway or that the United States is already locked in an information war with unidentified adversaries but rather that offensive information capabilities already exist that can cause significant disruptions in the US population by attacking inadequately protected information systems.

Simulations Suggest Malevolent Actors Could Do the Same

War-game simulations are also beginning to unmask the face of information conflicts and the problems associated with them. RAND created and presented a game to senior

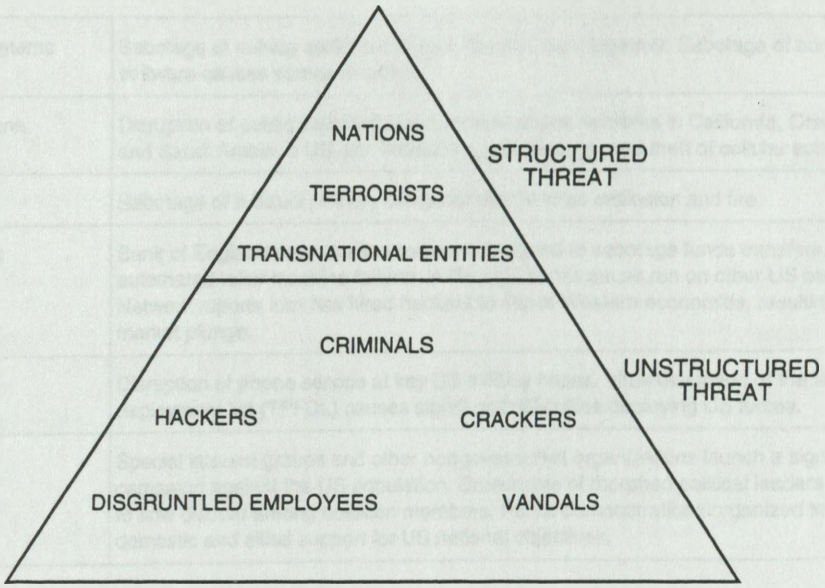


Figure 2.1. The Structured and Unstructured Threat

government officials during 1995, entitled "The Day After . . . in Cyberspace."[14] The game's information incidents, for the most part, reflect actual examples of information system failures (See appendix B, fig. B.2.). The game assumes the incidents occurred as the result of actions by malevolent actors. The scenario postulates information attacks against the US and its allies in the year 2000 by a resurgent Iran. Officials playing the game were tasked, in the form of recommendations to the president, to formulate national security policies to counter this new form of warfare.

The enemy pursued three general objectives in the RAND game. First, it launched against numerous US and allied targets multiple and varied information attacks that were designed to generate internal political pressures and erode popular confidence in the ability of governments to control the developing crises. Second, it targeted allied infrastructure and military centers of gravity in an effort to disrupt the coalition's ability to fight. Third, it used conventional theater military operations to distract national decision makers from its information operations against the United States. Figure 2.2 illustrates typical RAND targets and types of information attacks used against them (chap. 5 has an analysis of the RAND game; see appendix B for a full account of the game's highlights).

The enemy's information attacks blurred the distinction between the requirements of domestic law enforcement and the greater demands of a national security crisis. The players were ill prepared for this new dimension of warfare and were unable to agree on what was happening or how to defend against it. Decisive recommendations were difficult to generate and traditional military responses to rapidly changing events and nontraditional attacks were not effective.

Game participants, who were mostly senior government and DOD officials, failed to reach consensus regarding the seriousness of the threat with their assessments ranging

Transportation Systems	Sabotage of railway switches causes trains to slam together. Sabotage of commercial aircraft software causes planes to crash.
Telecommunications Systems	Disruption of public switching telecommunications networks in California, Oregon, Washington, and Saudi Arabia, a US ally. Monitoring, interference, and theft of cellular subscription numbers.
Power Sources	Sabotage of a Saudi refinery computer results in an explosion and fire.
Financial Systems	Bank of England detects alien software designed to sabotage funds transfers. Software-induced automated teller machine failures in Georgia banks cause run on other US banks. Cable News Network reports Iran has hired hackers to attack Western economies, resulting in US stock market plunge.
Military Forces	Disruption of phone service at key US military bases. Virus disruption of the time-phase force deployment list (TPFDL) causes significant difficulties deploying US forces.
Political Systems	Special interest groups and other nongovernment organizations launch a significant propaganda campaign against the US population. Broadcasts of morphed political leaders of US allies made to sow discord among coalition members. Public demonstrations organized to undermine domestic and allied support for US national objectives.

Figure 2.2. Targets and Types of Information Attacks

from "not a problem" to "couldn't be worse." The more time they spent on the problem, however, the more they considered it to be a difficult one that lacked concrete solutions and, in some cases, even starting points. In the end, most tended to describe the threat as one of greater magnitude than they had believed it to be before playing the game.

The Pentagon's DSB has reported the existence of vulnerabilities in the US information infrastructure that mirror those highlighted in the RAND war game. Vulnerabilities listed by the DSB and exploited in the RAND game include perception management of events or circumstances, deception, manipulation of information content or delivery, and the debilitation or destruction of information.[15] Echoing RAND's game scenario, the DSB also stated that activities and capabilities already exist that give cause for concern over the integrity of information systems that are key enablers of military superiority.[16] It notes that although there are limited efforts underway to detect and counter unstructured threats to US information systems, there is no nationally coordinated capability to detect, much less counter, a structured information attack by a determined adversary.[17]

Notes

1. Carl von Clausewitz, *On War,* ed. and trans. Michael Howard and Peter Paret (Princeton, N.J.: Princeton University Press, 1976), 75.

2. Ibid., 89.

3. United States, National Communications System, *The Electronic Intrusion Threat to National Security and Emergency Preparedness Telecommunications: An Awareness Document* (Arlington, Va.: National Communications System, 1994), 2–24.

4. Science Applications International Corporation (SAIC), *Planning Considerations for Defensive Information Warfare - Information Assurance* (Washington, D.C.: SAIC, 16 December 1993), 36.

5. United States Government Accounting Office (GAO), "Information Superhighway: An Overview of Technology Challenges," report to the Congress (Washington, D.C.: GAO, 23 January 1995), 37; also, Winn

Schwartau, *Information Warfare: Chaos on the Electronic Super Highway* (New York: Thunder's Mouth Press, 1994), 127.

6. Philip Elmer-DeWitt, "The Kid Put Us Out of Action," *Time,* 14 November 1988, 76.

7. Lawrence J. Haas, "NII Security: The Federal Role," draft (Washington, D.C.: National Information Infrastructure Security Issues Forum, 14 June 1995), 18.

8. Wayne Madsen, "Intelligence Agency Threats to Computer Security," *International Journal of Intelligence and Counterintelligence* 6 no. 4 (Winter 1993): 437–38; Leonard Lee, *The Day the Phones Stopped* (New York: Donald I. Fine, Inc., 1992); and Douglas Waller, "Onward Cyber Soldiers," *Time,* 21 August 1995, 44.

9. DOD, *1994 Defense Science Board Summer Study on Information Architecture for the Battlefield* (Washington, D.C.: Defense Science Board, 1994), 52.

10. Jeffrey Cooper, "Another View of Information Warfare: Conflict in the Information Age," draft (Washington, D.C.: Science Application International Corporation, 30 August 1995), 3.

11. Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the Twenty-First Century* (New York: Warner Books, 1993).

12. Cooper, 5.

13. Schwartau, 291.

14. RAND, "The Day After . . . In Cyberspace" (Santa Monica, Calif.: RAND, 1995), 33.

15. DOD, DSB, 28 and 51.

16. Ibid., 51.

17. Ibid., 25.

Chapter 3

New National Security Realities

The Commission considers the security of information systems and networks to be the major security challenge of this decade and possibly the next century . . . . We have neither come to grips with the enormity of the problem nor devoted the resources necessary to understand fully, much less rise to the challenge.

—Joint Security Commission Report to the Secretary of Defense and the Director of Central Intelligence, February 1994

Dramatic Technological Changes Have Produced New National Security Realities

Revolutionary developments in information technology are producing a revolution in military affairs that changes the realities upon which United States grand strategy is based. The following information age realities contribute to the foundation for a new grand strategy. These new realities are ordered and build upon each other:

- *Information technologies both modify the traditional spectrum of warfare and create a fifth dimension of conflict.* Revolutionary changes in warfare provide vast new opportunities with some liabilities—new strengths to be developed, new vulnerabilities to be protected, and new avenues to fulfill political ends.
- *Rapid exploitation of information can produce significant advantages in warfare and commercial competition.* Leaders who understand this new reality have the potential to get inside a competitor's decision-making cycle, seize the initiative in combat or commercial competition and thereby gain advantages over an opponent.
- *Information itself must be protected.* Reliance upon information systems to enhance decision cycles can become a liability if corrupted or destroyed data produce bad decisions. The places where data and information reside (databases, communication networks, logic programs) are alluring targets in a society heavily dependent upon them.
- As long as defensive countermeasures lag behind innovative uses of offensive information weapons, the US will have *new strategic vulnerabilities that make traditional notions of US physical sanctuary less meaningful.* US dependence upon information systems, combined with today's worldwide interconnectivity of computers has created an avenue for attack of strategic assets. While financial institutions, public switch networks, and power plants remain relatively safe from

crippling physical attacks, there is markedly less assurance that they are safe from information attacks because there are limited self-protection features in place.

- *Actors other than traditional nation-states can initiate information attacks.* Since the ante to enter information warfare is on a scale far below that of conventional warfare, potential attackers are not limited to traditional nation-states.
- If the US is to effectively build and execute a new grand strategy for national security, *new strategic measures of effectiveness are needed to prioritize both offensive and defensive efforts.*

These realities highlight the obsolescence of national security that plans a defensive grand strategy based solely upon conventional military forces. The Defense Department can no longer be the sole provider of national security. Defending information infrastructure, financial institutions, and other critical nodes from information attacks is beyond military authority and capability.[1]

Information Technologies Both Modify the Traditional Spectrum of Warfare and Create a Fifth Dimension of Conflict

I think it's appropriate to call information operations the fifth dimension of warfare. Dominating this information spectrum is going to be critical to military success in the future.

—Gen Ronald R. Fogleman
Chief of Staff of the Air Force

Information technologies have permanently modified the preexisting four dimensions (air, land, sea, space) of warfare. Desert Storm provided examples of this truth. Unparalleled information technologies produced greater weapon lethality and unprecedented clarity of the battlefield. The technologies that produced the lopsided victory continue to improve and are being driven not by military necessity but by commercial demand for improvements in information management.[2]

The nation's historic military leadership in technical development has ended. Commercial markets now influence deployment of advanced information technologies, and DOD finds itself following that lead.[3] DOD has become another consumer of information systems in a market driven by commercial imperatives rather than by the military's needs. This progress does not rest on congressional approval or disapproval of a defense budget but rather on a strong commercial market. Thus, not only will information technologies continue to expand but they will be sold rapidly throughout the world and many state and nonstate actors will choose to capitalize upon their potential as offensive weapons.[4]

Information technologies have done more than permanently alter conventional military forces—they have created a new dimension of conflict. General Fogleman and others have said that information dominance and winning information wars will be the prerequisite for victory in future conflicts.[5] Although Giulio Douhet made similar claims about airpower in the 1920s, his visionary projections of airpower failed to fully recognize the potential for countermeasures that would degrade airpower effectiveness. Whereas, airpower did revolutionize warfare, it was not to the extent of Douhet's visions. The information revolution will most likely run a similar course.

The United States is at the very beginning of a revolution in military affairs.[6] To understand this concept, it is important to distinguish between evolutionary and revolutionary change. In evolutionary change, progress is made by improving upon the last generation of military weapons, organizations, or tactics. It often takes the form of a seesaw battle between the development of new offensive capabilities followed quickly by the development of defensive countermeasures. First one is ascendant, then the other. Progress can be impressive but there still exists a continuity between the present and the past.[7]

Revolutionary change, on the other hand, results in almost no continuity between the present and the past. What we are seeing is something entirely new. Revolutionary changes are important because nations that recognize and exploit them usually defeat nations that do not.[8] Situations with the potential for revolutionary changes in warfare provide ambitious powers with an opportunity to become dominant or near-dominant powers.[9] Both Germany and Japan were medium-sized powers as rated by gross national product, population, and other broad measures of national power at the commencement of World War II. However, Germany's development of blitzkrieg and Japan's dramatic reliance upon carrier airpower provided each with significant advantages during the war's opening years. Indeed, it was not until 1942 that the Allies came to understand the significance of these two revolutionary developments in warfare and devised measures to counter them. The United States is once again faced with revolutionary change and, as it has in the past, such change could once again pose a threat to the nation.[10]

The concept of using information and information technology as a weapon is at the heart of the current revolution in military affairs. Until the United States understands this basic change in war fighting and devises appropriate countermeasures to defend itself, it will be vulnerable to actors who more quickly grasp the nature of this change and seek to exploit it. At present, the US defense establishment remains unchallenged in the four traditional dimensions of warfare. However, the defense establishment will not likely be the primary defense mechanism in the fifth dimension—the information realm.

Information warfare as a new dimension of conflict provides unprecedented methods to directly impact a nation's will through information attacks that can circumvent many conventional military defenses. It will produce new forms of warfare quite different from the other four dimensions of conflict. The Air Force pamphlet, *The Nation's Air Force Booklet,* states, "Today, dominating the information spectrum has become as critical to conflict as occupying the land or controlling the air has been in the past."[11] Superimposed across the traditional spectrum of warfare, information not only complements existing dimensions of warfare but itself creates a new dimension for exploitation. It represents yet another means of achieving political objectives.

Rapid Exploitation of Information Can Produce Advantages

History does not teach that better technology necessarily leads to victory. Rather victory goes to the commander who uses technology better, or who can deny the enemy his technology.

—Office of the Chief of Naval Operations

Decision-making cycles tighten in the Information Age. Information delivers enormous power into the hands of any individual, anywhere on the globe, with the wits

and interest to use it. Those who understand this new reality have the potential to get inside a competitor's decision-making cycle and seize the initiative in combat or competition.

This has obvious benefits in warfare and commercial applications. These new technologies provide users with the potential to rapidly: (1) *Observe* with greater detail the reality of their environment; (2) *Orient* themselves with greater accuracy than someone with less information; (3) *Decide* with greater insights and, thereby, greater accuracy; and (4) *Act* within a shorter time span and with enhanced assertiveness.[12] This four-step paradigm, entitled the *OODA loop*, is one way of viewing decision cycles. Leaders (both civilian and military) who can effectively observe, orient, decide, and act faster than their opponent can seize the initiative in combat or competition and shape the battlefield by limiting and channeling an adversary's options. One writer called the US military's breathtaking speed in completing Desert Storm OODA loops "a sort of continuous temporal outflanking."[13]

This facet of OODA enhancement places greater pressures on senior leaders to respond rapidly to changing conditions throughout the world. Shortened time lines for decision making are particularly significant in the arena of national security where today's decision makers, and those surrounding them, have a limited understanding of warfare or the capabilities of the military.[14] They also represent potential liabilities if the four-step OODA cycle is interrupted or a decision maker is forced to decide or act without adequate time to observe and orient. When British prime minister John Major was asked if leaders today are disadvantaged by the "CNN Syndrome" and if the demand for immediate response concerned him, he replied,

> It doesn't get on my nerves. It is a fact of life. I think it is bad for government. I think the idea that you automatically have to have a policy for everything before it happens and respond to things before you have had a chance to evaluate them properly isn't sensible.[15]

Presidential advisor George Stephanopoulis echoes Prime Minister Major's sentiments:

> In the White House . . . we have 24-hour news cycles . . . CNN assures that you are forced to react at any time, and that's going to happen throughout the time of the Clinton presidency.[16]

The national security advisor to former vice president Dan Quayle was more specific:

> There's really no time to digest this information so the reaction tends to be from the gut, just like the reaction of the man on the street. High level people are being forced essentially to act and to formulate responses or policy positions on the basis of information that is of very uncertain reliability.[17]

Using information technology to create advantages for decision makers by compressing the amount of time needed to gather data is an important advantage in warfare. Unless the data collected is free from contamination, however, it may also be a potential liability. Moreover, the same technology may be used to place an opponent at a disadvantage by forcing it to make rapid decisions based upon corrupted data. These concepts of speed and accuracy in decision making reveal the importance of protecting information.

Information Itself Must Be Protected

Know the enemy and know yourself; in a hundred battles you will never be in peril.

—Sun Tzu

A generally accepted information hierarchy (fig. 3.1) illustrates the importance of protecting information. At the bottom of this hierarchy are data that are defined as raw facts. It may include useful or irrelevant and redundant facts and must be processed to become meaningful. Information consists of the trends or patterns that emerge from quantities of processed data. The third layer is knowledge of the information provided, the circumstance of attempting to discern the truth through reasoning. Finally, there is wisdom, the epitome of the information hierarchy. Wisdom comes with gaining insight from knowledge.[18]

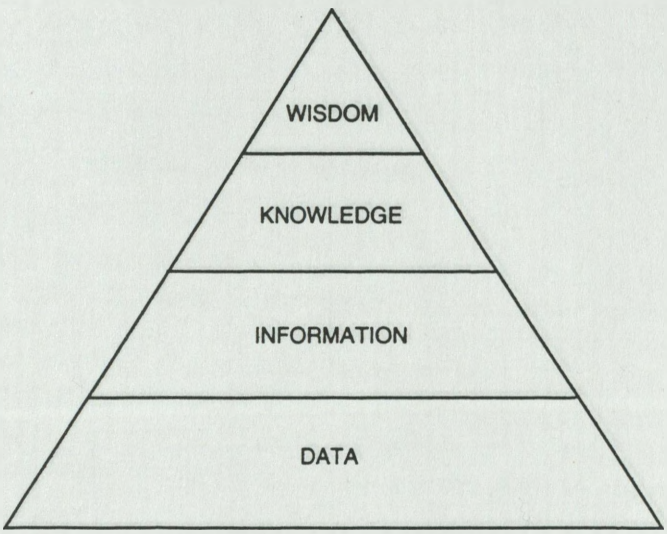


Figure 3.1. Information Hierarchy

These four levels of the information hierarchy (fig. 3.1) relate to the OODA decision-making cycle (fig. 3.2). Data requires observation, then orientation to become information. Decision makers must then study the available information and apply reason to acquire knowledge. From such knowledge, hopefully, wise decisions are made.*[19]

Corrupting either of the two bottom elements inevitably taints the elements above them and impacts the OODA decision-making cycle. Therefore, protection of data and information becomes critical to the integrity of knowledge and wisdom and to the accuracy and appropriateness of decision making.

---

* Col John Boyd said that the most important part of the OODA loop is the orient phase. Orientation is the real starting point because it affects what we decide to observe and then what we decide to do based on what we observe.

Information Itself Must Be Protected

Know the enemy and know yourself; in a hundred battles you will never be in peril.

—Sun Tzu

A generally accepted information hierarchy (fig. 3.1) illustrates the importance of protecting information. At the bottom of this hierarchy are data that are defined as raw facts. It may include useful or irrelevant and redundant facts and must be processed to become meaningful. Information consists of the trends or patterns that emerge from quantities of processed data. The third layer is knowledge of the information provided, the circumstance of attempting to discern the truth through reasoning. Finally, there is wisdom, the epitome of the information hierarchy. Wisdom comes with gaining insight from knowledge.[18]

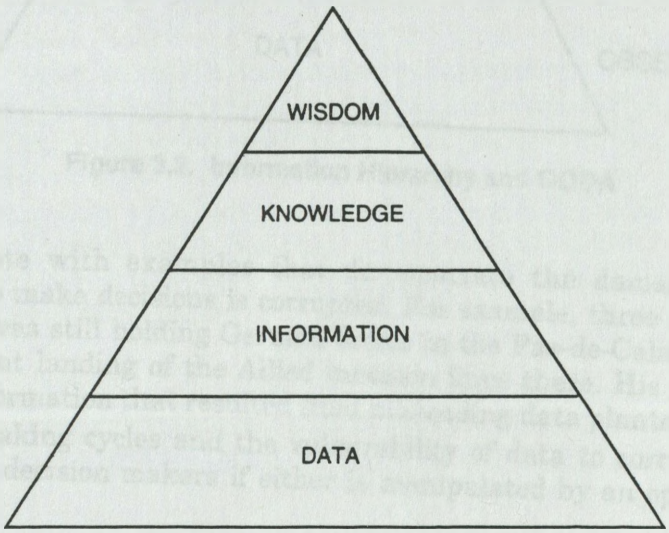


Figure 3.1. Information Hierarchy

These four levels of the information hierarchy (fig. 3.1) relate to the OODA decision-making cycle (fig. 3.2). Data requires observation, then orientation to become information. Decision makers must then study the available information and apply reason to acquire knowledge. From such knowledge, hopefully, wise decisions are made.*[19]

Corrupting either of the two bottom elements inevitably taints the elements above them and impacts the OODA decision-making cycle. Therefore, protection of data and information becomes critical to the integrity of knowledge and wisdom and to the accuracy and appropriateness of decision making.

---

* Col John Boyd said that the most important part of the OODA loop is the orient phase. Orientation is the real starting point because it affects what we decide to observe and then what we decide to do based on what we observe.

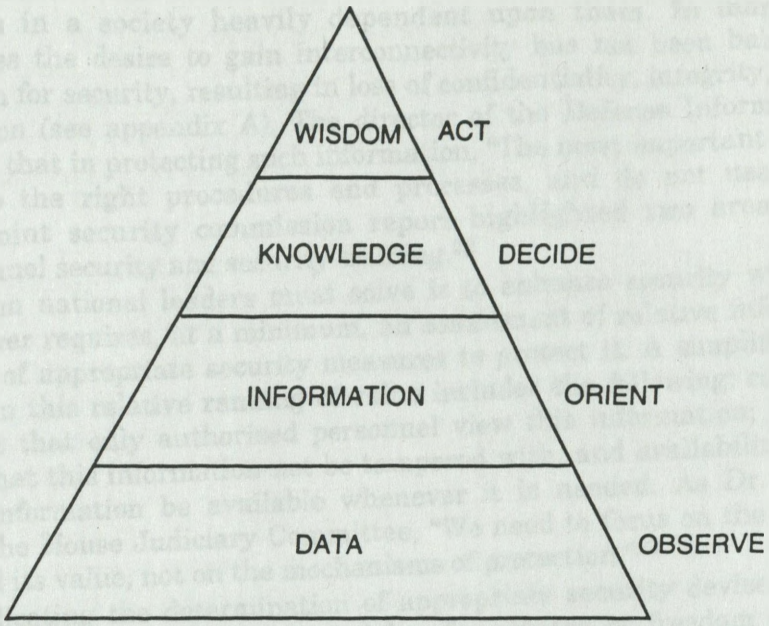


Figure 3.2. Information Hierarchy and OODA

History is replete with examples that demonstrate the damage done when the information used to make decisions is corrupted. For example, three days after D day in Normandy, Hitler was still holding German forces in the Pas-de-Calais area to repel the supposedly imminent landing of the Allied invasion force there. His decision was based upon inaccurate information that resulted from misleading data planted by the Allies.

Rapid decision-making cycles and the vulnerability of data to corruption underscores the vulnerability of decision makers if either is manipulated by an opponent. As George Stein puts it:

> Information warfare is about the way humans think, and more importantly, the way humans make decisions. . . . It is about influencing human beings and the decisions they make. . . . Information warfare is real warfare, it is about using information to create such a mismatch between us and an opponent that, as Sun Tzu would argue, the opponent's strategy would be defeated before his first forces can be deployed or his first shots fired. The target of information warfare, then, is the human mind, especially those minds that make the key decisions . . . on if, when and how to employ assets and capabilities embedded in their strategic structures.[20]

The traditional method of guarding information is to limit physical access to it. The locked file cabinet and personal security clearances are products of current thinking about how to best limit the number of persons with the ability to peruse and use confidential or sensitive information. However, the Information Age is dramatically changing this equation and requires a change in our cultural thinking about security.

Modern information technology places a premium on electronic transmittal, processing, and storage of information. America's wholehearted embrace of information technology has transferred huge quantities of private and sensitive information from the locked file cabinet onto computer files accessible through information networks. The places where

data and information reside (databases, communications networks, logic programs) are alluring targets in a society heavily dependent upon them. In many significant, documented cases the desire to gain interconnectivity has not been balanced with an adequate concern for security, resulting in loss of confidentiality, integrity, or availability of the information (see appendix A). The director of the Defense Information Systems Agency observed that in protecting such information, "The most important way is making sure people use the right procedures and processes, and do not use shortcuts [in security]."[21] A joint security commission report highlighted two areas for security emphasis: personnel security and security training.[22]

The conundrum national leaders must solve is to enhance security without limiting access. The answer requires, at a minimum, an assessment of relative information value and assignment of appropriate security measures to protect it. A simplified look at the issues involved in this relative ranking of value includes the following: confidentiality—how critical is it that only authorized personnel view this information; integrity—how important is it that this information not be tampered with; and availability—how crucial is it that this information be available whenever it is needed. As Dr. James Hearn testified before the House Judiciary Committee, "We need to focus on the information to be protected, and its value, not on the mechanisms of protection."[23]

Further complicating the determination of appropriate security devices are issues of liability, public affairs, legality, personal rights for privacy or freedom of speech, and national security. Each of these frames of reference provide potentially different answers to the same set of questions. There must be a balance between the needs of the state and the rights of the individual, between the need to know and the need to maintain privacy.[24] Such an exercise highlights the importance of a national security grand strategy built upon a consensus around these issues.

New Strategic Vulnerabilities Have Made Traditional Notions of US Physical Sanctuary Less Meaningful

There is no geography or sanctuary in cyberspace.

—Vice Adm Arthur Cebrowski
United States Navy

The permeability of worldwide information systems reduces the relevance of the physical sanctuary that our nation has enjoyed for more than 200 years. Since its founding, the United States has rested safely behind the Atlantic and Pacific oceans—its strategic centers of gravity safely protected by physical barriers. Since the end of World War II, standing conventional forces and a policy of deterrence have maintained this protective barrier even from the nuclear threat of the cold war. Now, in this new dimension of warfare, physical sanctuary and reliance upon conventional military forces will not protect many US strategic centers of gravity from potential information attacks. As long as defensive countermeasures of information warfare lag behind innovative uses of the same technology, the US will have new strategic vulnerabilities.

For the time being, information technology holds the potential to become a great equalizer among nations. The efforts of vulnerable nations, a list the US tops, to create defensive countermeasures to information attacks will directly impact both the depth of such attacks as well as the number of potential information attackers. The window of vulnerability is only as big as those who are vulnerable allow it to be.

Actors Other Than Traditional Nation-States Can Initiate Information Attacks

Who are those guys?

—Butch Cassidy and the Sundance Kid, 1969

When considering the nature of the threat, cold war mentality and measurement devices must be discarded. Information warfare can be executed with far less capital than is needed for conventional conflicts. Large-scale conventional warfare requires taxing the resources of large populations to build the force structure; thus, only nation-states have had the wherewithal to engage in it. Additionally, conventional warfare requires greater force structure and training expense than does the smaller elite cadre required of information warfare. Since the ante to enter information warfare is on a scale far below that for conventional warfare, potential attackers are not limited to traditional nation-states. One view is that anyone with an agenda, a modicum of training, and a small investment in equipment can launch an information attack.[25] Others disagree. However, although estimates needed to mount significantly disruptive attacks against information targets may vary, there is general consensus that the amount is well within the range of nonstate actors, including groups and individuals.[26]

The emergence of these nonstate actors represents perhaps the most significant threat to US national security interests in the foreseeable future. They could potentially launch an invisible electronic attack against the US without a shot being fired and without direct knowledge of who the adversary might be.[27]

New Strategic Measures of Effectiveness Are Needed to Prioritize Both Offensive and Defensive Efforts

Three elements determine the effectiveness of a national strategy. What is the strategic goal? How well is national power oriented to achieve the goal? What do the indicators show with respect to how well the nation is doing in achieving its goal? The answers to these questions, taken together, establish the planned measure of strategic effectiveness.[28] None exists for Information Age conflict strategies for either offensive or defensive information warfare.

It is important to differentiate between measures of effectiveness at the operational and strategic levels. The military may perform well at the operational level, but fail because those operations are not linked to a strategic goal. US military operations in

Vietnam were an example of this disconnect. Talking to a senior North Vietnamese official after the war, a US Army officer observed that the United States military had never been defeated in combat. His North Vietnamese counterpart replied that while that was true, it was also irrelevant.[29] The North Vietnamese officer was correct.*

Attrition is the strategic measure of effectiveness for traditional warfare. Presently, nations gauge progress toward achieving their war aims by measuring numbers of enemy killed, amounts of supplies destroyed, extent of the enemy infrastructure rendered unusable, transportation disrupted, and so forth. The ultimate goal of attrition warfare is to destroy the enemy's will to make war by destroying its physical war-making capabilities. However, this measure of strategic effectiveness is inapplicable when the weapons used are not designed to bring about physical destruction. The effectiveness of information as a weapon cannot be measured readily by resorting to attrition methodologies. New measures of strategic effectiveness must be designed to assess both offensive and defensive information warfare.

Looking at the Vietnam War from North Vietnam's standpoint, one can argue that it is a good example of information warfare at the strategic level. It is logical to assume, particularly after the 1968 Tet offensive, that North Vietnam could not hope to defeat the United States militarily on the battlefield. That did not mean, of course, as subsequent events proved, that North Vietnam was defeated—quite to the contrary. The effectiveness of the North's strategy was not measured in terms of attrition warfare but rather by the weakening of America's resolve to continue the struggle. They succeeded because they linked what national power they possessed to their strategic goal and focused all of their energies on attaining it.** But what indicators did they use to determine whether they were making progress? The number of antiwar newspaper articles? The size and fervor of American antiwar demonstrations? The speeches of antiwar politicians? Were these measures somehow formalized or simply a consensus of the gut feelings of North Vietnam's Politburo members?

Warfare in the Information Age requires new measures of strategic effectiveness that account for the impact of information technology on the enemy's leaders, government, and population. The lack of these measures is a new reality that must be addressed by national security policy makers.

Synopsis of Information Age Realities

These six realities point to the fact that the grand strategy of national security built solely on conventional forces is out of date. The Department of Defense can not be the sole

---

* In 1995, Christopher Jenner interviewed Gen Nguyen Don Tu, an intelligence officer in the North Vietnamese army, who served as Gen Dong's chief of staff during the 1968 Tet campaign on Hue, and was also a member of the North's negotiation team at the Paris peace talks. Gen Tu was author of a report, "How to Manipulate the U.S. Media." His knowledge of US political systems and civilian sensitivity was telling and he provided sound evidence of having put this to great effect in information warfare with the United States in the Vietnam War. During an oral history interview of Maj Gen Edward Lansdale in 1986, Mr. Jenner learned of Gen Tu and of his manipulation paper, that was subsequently distributed to a number of communist countries, including Cuba. Maj Gen Landsdale held Gen Tu in high esteem as an adversary and considered him a brilliant information warfare exponent.

** Today, information technology would present the North Vietnamese with additional options to directly impact the weakening of US resolve.

providers of national defense in the Information Age. *Information technologies have created a fifth dimension of conflict.* Recognizing the uniqueness of this dimension highlights the limited relevance of the world's most powerful army, navy, and air force in defending strategic centers of strength from information attacks. The sum of their conventional forces is far more potent than any would challenge conventionally, but are an inadequate deterrent to deflect information weapons or protect information targets. In this new dimension, the *rapid exploitation of information can produce significant advantages in warfare and in commercial competition.* Leaders who exploit information technology may seize the initiative, get inside an opponent's decision-making cycle, and thereby limit or channel the options available to the enemy. Moreover, in the Information Age interconnectivity and dispersed computing power have greatly expanded access and dependence upon information, making the places it resides (databases, communication networks, logic programs) more susceptible and attractive targets. Therefore, *information itself must be protected.* Information can be used as a weapon to corrupt or destroy or it can be the target of an attack. For as long as defensive countermeasures lag behind innovative use of offensive information weapons, the United States will have *new strategic vulnerabilities that make traditional notions of US physical sanctuary less meaningful.* Heavy US dependence upon information systems combined with today's worldwide interconnectivity of computer systems, which have limited self-protection features, has created an avenue for attack of strategic assets. Financial institutions, public switch networks, power plants, and other strategic centers of strength could be at risk from information attacks, and military conventional forces can do very little to protect them. Ample historical examples exist, demonstrating the significant disruptions of information systems that can occur. Although many of these have been caused by computer logic errors, this does not preclude malevolent actors from intentionally seeking to cause such havoc to further a particular cause. Additionally, since the ante to enter information warfare is on a scale far below that for conventional warfare, *potential attackers expand far beyond traditional nation-states.* If the United States is to effectively build and execute a new grand strategy for national security, efforts beyond the military must be employed and *new strategic measures of effectiveness are needed to prioritize both these efforts in both the offensive and defensive categories.*

The following chapters build a proposal for a new strategic framework upon this foundation—an information-age framework from which a new grand strategy for national security can be crafted.

Notes

1. Science Applications International Corporation (SAIC), *Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance* (Washington, D.C.: SAIC, 1995), 2-19, 2-20, 4-1. The Computer Security Act of 1987 assigned responsibility for security standards and guidelines to the Department of Commerce, National Institute of Standards and Technology, National Security Agency, and General Services Administration. Executive Order 12356 established the Information Security Oversight Office, under the Office of Management and Budget, to oversee compliance with national security information guidance. Protection of civilian infrastructure by the Department of Defense is further complicated by the Posse Comitatus Act which limits the use of the military for enforcing the law of the land.

2. Kenneth C. Allard, "The Future of Command and Control: Toward a Paradigm of Information Warfare," *Turning Point: The Gulf War and US Military Strategy,* ed. L. Benjamin Ederington and Michael J. Mazaar (Boulder, Colo.: Westview Press, 1994), 161–92.

3. SAIC, 4-1.

4. Ibid., 4-2.

5. Lt Gen John S. Fairfield, "A Jointly Focused Vision," *Armed Forces Journal* 133, no. 6 (January 1996): 37; United States Army, *Concept for Information Operations* (Fort Monroe, Va.: TRADOC, August 1995), 7; Gen Ronald R. Fogleman, "Information Operations: The Fifth Dimension of Warfare," address, Armed Forces Communications-Electronics Association meeting, Washington, D.C., 25 April 1995.

6. Andrew W. Marshall, memorandum for the record, subject: RMA Update, 2 May 1994.

7. Richard J. Dunn III, *From Gettysburg to the Gulf and Beyond: Coping with Revolutionary Technological Change in Land Warfare* (Washington, D.C.: Institute for National Strategic Studies, McNair Paper 13, 1992), 3.

8. Dunn, 3; Jeff Barnett, "The Revolutions in Military Affairs," briefing slides (Washington, D.C.: Office of Net Assessment, 1995).

9. Paul Wolfowitz quoted in Marshall, 3.

10. Dunn, 3.

11. United States Air Force, *The Nation's Air Force Booklet* (Washington, D.C.: US Air Force, 1995), 11–12.

12. Col John R. Boyd, "A Discourse on Winning and Losing," briefing slides (Maxwell AFB, Ala.: Air University Library, August 1987).

13. Oliver Morton, "The Information Advantage," *The Economist,* 10 June 1995, 5.

14. James Adams, "The Role of the Media," lecture, Information Warfare Course, National Defense University, Washington, D.C., 17 December 1995.

15. Thomas Plate and William Tuohy, "John Major; Even Under Fire, Britain's Prime Minister Holds His Own," *Los Angeles Times,* 20 June 1993, sec. M.

16. David S. Broder, "Looking Ahead in '92," *Boston Globe,* 6 April 1994.

17. Carnes Lord, remarks recounted in Thomas J. McNulty, "Television's Impact on Executive Decisionmaking and Diplomacy," *The Fletcher Forum of World Affairs* 17 (Winter 1993): 81–82.

18. John Arquilla and David Ronfeldt, "Information, Power, and Grand Strategy: In Athena's Camp," paper, Catigny Conference, Wheaton, Ill., July 1995, 6. The authors cite as the source of the diagram in Harlan Cleveland, *The Knowledge Executive: Leadership in an Information Society* (New York: Truman Talley Books, 1985); Robert Lucky, *Silicon Dreams: Information, Man and Machine* (New York: St Martin's Press, 1989); and David Ronfeldt, *Cyberocracy, Cyberspace and Cyberology: Political Effects of the Information Revolution* (Santa Monica, Calif.: RAND, 1991), 4.

19. United States Army Field Manual (FM) 100-6, "Information Operations, " draft (Fort Monroe, Va.: TRADOC, January 1996), 2-1, 2-2, 2-3, 4-1, 4-2, 4-3, 4-4; for same conclusion, see also Col Edward Mann, *Thunder and Lightning: Desert Storm and the Airpower Debates* (Maxwell AFB, Ala.: Air University Press, April 1995), 152; Gen Frederick M. Franks, address, Association of the United States Army Symposium, Orlando, Fla., 8 February 1994.

20. George Stein, "Information Warfare," *Airpower Journal,* Spring 1995, 32.

21. Lt Gen Albert Edmonds, interview, *Defense News,* 16–22 October 1995, 102.

22. Joint Security Commission, *Redefining Security: A Report to Secretary of Defense and Director of Central Intelligence* (Washington, D.C.: Joint Security Commission, February 1994), vi.

23. Congress, House Judiciary Committee, "The Threat of Foreign Economic Espionage to US Corporations," testimony by Dr. Hearn, 29 April–7 May 1992, Washington, D.C.: Government Printing Office, 1992, 87.

24. SAIC, 4-1.

25. Ronald Grove, "The Information Warfare Challenges of a National Infrastructure," paper, InfoCon symposium, Washington, D.C., September 1995, 9.

26. Roger C. Molander, Andrew S. Riddile, and Peter A. Wilson, "Strategic Information Warfare: A New Face of War," draft (Santa Monica, Calif.: RAND, 1995), xvi; DOD, DSB, 52.

27. SAIC, 2-66.

28. Stephen P. Rosen, *Winning the Next War: Innovation and the Modern Military* (Ithaca, N.Y.: Cornell University Press, 1991), 35.

29. Harry G. Summers, *On Strategy: A Critical Analysis of the Vietnam War* (Novato, Calif.: Presidio Press, 1982), 1; Christopher Jenner, memorandum to authors, March 1996. Notes from Christopher Jenner regarding personal interview with Gen Nguyen Don Tu, 1995; and an oral history interview of Maj Gen Edward Lansdale in 1986.

Chapter 4

A Strategic Framework

Col John A. Warden III, USAF, retired, a modern strategic thinker, asserts that today's industrial nations must be viewed as systems that derive their national power from five centers of gravity, each of which is critical to the state's existence.[1] Combined, they produce a synergy from which national power emerges. According to Warden, modern strategic warfare must focus on this system as a whole with the purpose of forcing changes in one or more of its centers of gravity. Such changes, he contends, will produce disruptions in the nation as a system and lead to changes in its policies or to its physical inability to continue resistance.[2] Like Clausewitz, Warden believes the purpose of war is to compel the enemy's submission.

Centers of Gravity: Nation-States Viewed as Systems

Warden's centers of gravity, also depicted in figure 4.1, consist of the following:

- A nation's *leaders,* civilian or military, who have the authority to commit their country to war, prolong its resistance, or lead it to peace.
- *System essentials* are the resources or facilities without which a nation cannot maintain itself. They are not necessarily defense related or contained within the boundaries of a nation. In many cases they may be the most critical nodes within these resources or facilities.*
- The *infrastructure* consists of a nation's system for moving goods and services. Roads, bridges, airports, rail lines, and ports all fall within this category. This also contains portions of a nation's industry that are not considered system essentials.
- A nation's *population.* A nation's citizens, whether within or outside of the nation's borders.**
- The *defense mechanism* consists of military forces. The nation's defense systems protect the nation from external and internal threats. They also shield other centers of gravity from attack and threaten the centers of gravity of competitor states. They include law enforcement and intelligence agencies.

---

* Warden places telecommunications in the leadership ring. We have elected to place it in the system essentials category.

** As Clausewitz, Sun Tzu, Churchill, and Ho Chi Minh knew, and as restated by Gen Vo Nguyen Giap, "In war there are two factors, human beings and weapons. Ultimately though, the human beings are the deciding factors." This lesson has been learned by US opponents in Bosnia, Libya, Iran, and Iraq.

Leadership	System Essentials	Infrastructure	Population	Defense Mechanism
Government National Leadership (National Command Authorities, Congress, Cabinet)	Critical nodes of telecommunications systems, power and petroleum distribution systems, financial system, trade	Transportation systems, research and development facilities, key production, media, retail, health, education, entertainment	Citizens	Military forces, Law enforcement agencies, intelligence activities

Figure 4.1. The Nation as a System, Depicting a Nation's Five Strategic Centers of Gravity as a Matrix

The Relative Importance of Strategic Centers of Gravity

Depicting a nation's centers of gravity as five concentric circles, or strategic rings, illustrates their relative importance (fig. 4.2). At the center of this model is the nation's leadership. It occupies the most protected position because it alone can make the decisions that lead a country into or away from war. Surrounding it, in descending order of importance, are system essentials, the infrastructure, and the population. The outermost strategic ring, the defense mechanism, is the most resistant to attack and acts as an outer shell. Its function is to guard and protect the other strategic rings from external attack or degradation and to promote the nation's policies by threatening the strategic rings of competitor nations.[3] The outermost, or military ring, is the most important center of gravity in conventional warfare because it protects the other more vulnerable centers. Once the military ring is penetrated, a nation's inner core becomes exposed and its leaders face a Hobson's choice of either submission or annihilation. Accordingly, for disciples of Clausewitz, the objective of violence is to disarm an enemy's military forces.

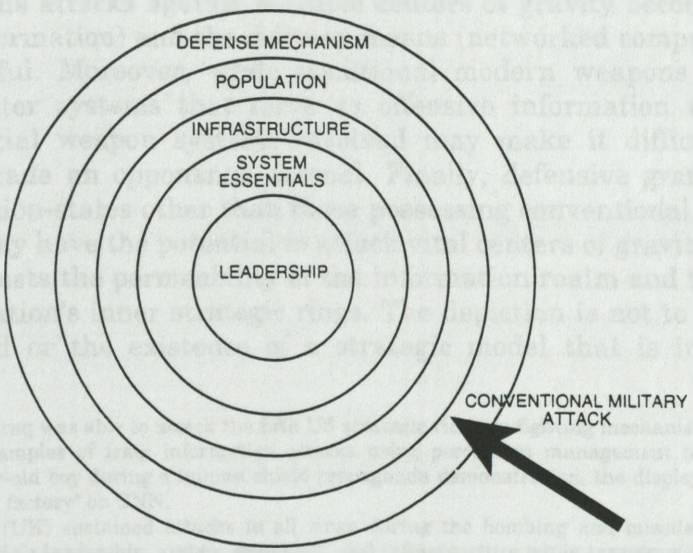


Figure 4.2. Warden's Strategic Rings

The Fifth Dimension Presents Both Opportunities and Vulnerabilities

Permeability and access characterize the fifth dimension and present strategic planners with new opportunities, new vulnerabilities, and new grand strategy options. Comprehending what is new requires an understanding of what has changed. In the past, nation-states conducted military operations in four dimensions (land, sea, air, and space) to reach the enemy's internal strategic rings (fig. 4.2). Evolving weapons technology has provided a limited ability to leapfrog an enemy's protective outer shell on occasion and directly attack its more critical centers of gravity.* In response, nations have constructed more physical barriers in the skies and in space in the form of air and missile defenses. These provide a reasonable measure of protection against traditional attacks. In most instances, these defenses, along with constraints in time, space, or resources, prevent a nation from effectively attacking more than one or two of an enemy's strategic rings.[4]

Time, space, and resources are also constraints in a military campaign (a series of related military operations aimed at accomplishing a strategic or operational objective within a given time and space).[5] Amassing the amount of conventional hardware and delivery systems necessary to launch simultaneous attacks against all five strategic rings is difficult, if not prohibitive. A result is that nations fighting in the four existing dimensions of warfare husband their war-fighting assets, assess enemy vulnerabilities, and carefully prioritize targets for attack. This prioritization makes the outermost strategic ring, the fighting mechanism, paramount as a target, because as long as it remains a viable fighting force that can protect the state's more vital centers of gravity, the nation cannot be subdued.

The permeability of traditional defense mechanisms to information attack, with the consequent increase in access to enemy strategic centers of gravity, has significant ramifications for planners of grand strategy. Physical defeat of an enemy's military forces may no longer be necessary to gain direct access to its more vulnerable inner strategic rings. Simultaneous attacks against multiple centers of gravity become possible because the weaponry (information) and the delivery means (networked computers) are relatively cheap and plentiful. Moreover, while traditional modern weapons remain capable of destroying computer systems that serve as offensive information weapons, the sheer number of potential weapon systems involved may make it difficult to eliminate or substantially degrade an opponent's arsenal. Finally, defensive grand strategists must take note that nation-states other than those possessing conventional military power and nonstate actors may have the potential to attack vital centers of gravity.

Figure 4.3 suggests the permeability of the information realm and the increased access it provides to a nation's inner strategic rings. The depiction is not to suggest that access will be unopposed or the existence of a strategic model that is indefensible. On the

---

* During the Gulf War, Iraq was able to attack the fifth US strategic ring, its fighting mechanism, the only ring to which it could obtain access. Examples of Iraqi information attacks using perception management techniques include Saddam Hussein's use of a 7-year-old boy during a human shield propaganda demonstration, the display of civilian casualties, and the destroyed "baby milk factory" on CNN.

The United Kingdom (UK) sustained attacks to all rings during the bombing and missile attacks in World War II. Germany damaged Britain's leadership, system essentials, and infrastructure while targeting its fourth strategic ring, the population.

contrary, as previously noted, the capability of an opponent to successfully penetrate to strategic centers of gravity with information weapons will depend upon the vigilance and defenses of the targeted nation. The development of effective countermeasures is likely to be the product of first recognizing the threat and then developing appropriate defenses. The danger to the United States's centers of gravity lies in the period before such countermeasures are in place.

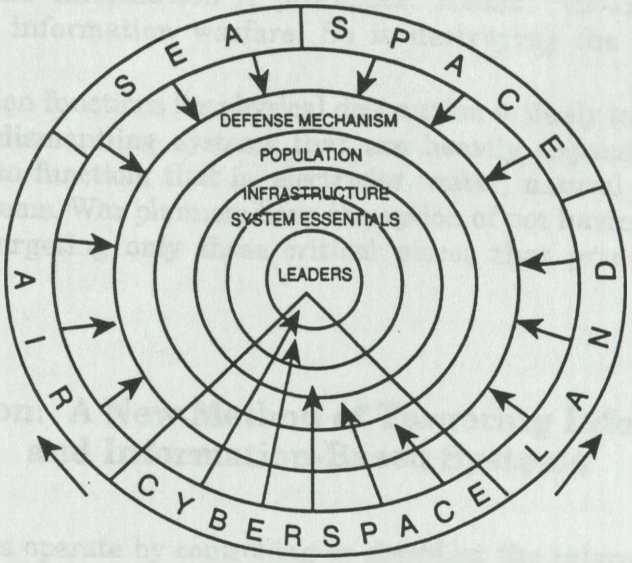


Figure 4.3. The Fifth Dimension of Warfare

Weapons for Attacking the Intangible

Information weapons attack targets in three ways: physical destruction, alteration of the target's internal operating logic, and manipulation of the target to produce behavioral changes. For ease of reference, these three categories are called destruction, corruption, and perception management.[6]

Physical Destruction Remains a Means of Attack

Attacks using conventional weapons systems remain important strategically because they target physical assets of the enemy's strategic centers of gravity. In the

Weapons Category	Weapons Function	Weapons Type
Destruction	Physical destruction of targets	Conventional

Figure 4.4. Physical Destruction Attacks the Electronic Components of a Nation's Information Systems

information realm, they destroy the electronic components of information systems, that is, switches, trunk wires, major databases, and other key physical information nodes (fig. 4.4).[7]

Though iron bombs themselves are not normally perceived as information weapons, it is important to remember that it is their effects upon the target that concern us, not their technical capabilities. If successful, iron bombs against an information node deny the enemy use of the information it processes. Hence, "(B)ombing a telephone switching facility is information warfare. So is destroying the switching facility's software."[8]

Targeting information functions for physical destruction is likely to produce new attack strategies aimed at dismantling systems that are heavily dependent upon electronic information systems to function, that is, electricity, water, natural gas, transportation, and broadcasting systems. War planners have the option of not having to target an entire system but rather targeting only those critical pieces that process the information controlling it.

Corruption: A New Method of Targeting Information and Information-Based Systems

Corruption weapons operate by controlling or disabling the internal operating logic of the targeted networks and systems (fig.4.5).[9]

Viruses, chipping, sniffers, high energy radio frequency (HERF) guns, Electro-Magnetic Pulse Transformer (EMP/T) bombs, their numerous variants, and mutations all fall within this category.[10] These weapons are important because they control an enemy's information systems by controlling their internal operating logic. Such control means control of an enemy's decision-making process and of his awareness and understanding of his environment.[11] Physical destruction of these systems, with the concomitant need to reconstruct them at war's end, is no longer required. Given the devastating power of modern weapons systems, defeat of an enemy without inflicting massive collateral damage that inhibits the enemy population's ability to sustain itself is much preferred to the costs of rebuilding a country following its destruction from traditional attacks.

Weapons Category	Weapons Function	Weapons Type
Corruption	Disruption of internal operating logic	Viruses of all types, high energy radio frequency (HERF) guns, ElectroMagnetic Pulse Transformer (EMP/T) bombs, filters, and agents

Figure 4.5. Corruption Alters the Internal Operating Logic of the Targeted Networks and Systems

Perception Management: Improved Means of Targeting a Population

Perception management seeks to affect what an opponent's targeted information systems portray as reality (fig. 4.6).[12] In some respects, it is analogous to the effects produced by psychological or deception operations. However, the access that modern information technology provides to enemy centers of gravity has made it much more.

Perception management can be clandestine or open, manipulative or straightforward. It can occur over an extended period of time or during an instant, perhaps at the critical moment during a crisis. It can be broad based or targeted with the precision of a rifle shot. It presents both great opportunities and great vulnerabilities. Selective spamming,* spoofing,** and misinformation are examples of perception management operations seeking to portray information as other than what it actually is.[13] The objective is usually short term and likely to be a specific decision or decision maker.

Slogans, promulgating specific arguments, injecting favorable points of view into public discourse and media manipulation (the "CNN factor"***) are open forms of perception management the effects of which are likely to be longer lasting. Precipitous swings in public sentiment, produced by the emotional closeness of watching dramatic events, are increasingly driving the national agenda as political leaders shift from one crisis or controversy to the next. Accelerated decision-making cycles increase the chances of serious mistakes as people struggle to deal with increasingly complex matters during shorter time frames.

The importance of perception management is growing. Information technology is changing the world from one in which information control was relatively easy to one in which it is now virtually impossible. This change has had corrosive effects upon hierarchical institutions and governments that have relied, in whole or in part, upon control of information to maintain their status in the existing order.[14] Communism collapsed, in part, because the information revolution forced its governments to face a choice between openness and the possibility of their own demise or perpetual economic impoverishment and increasing civil upheaval.[15]

Weapons Category	Weapons Function	Weapons Type
Perception Management	Behavior	Spamming, spoofing, misinformation, discourse, slogans, arguments, information overload

Figure 4.6. Perception Management Affects What an Opponent's Targeted Information Systems Portray as Reality

* Using technology to "take over" a broadcast and replace the images shown with one's own program.

** Electronically altering images or words to convey a meaning other than intended by the subject being filmed or photographed.

*** America has recently experienced the "CNN factor," increasing the public's emotional participation by showing dramatic events for spectators' direct viewing. The result can be a loss of viewer objectivity.

Centers of Gravity and Weapons Categories Form a Basic Framework

A nation's five strategic centers of gravity (fig. 4.1) and the classification of weapon systems by function (figures 4.4, 4.5, and 4.6) provide the basic data needed to begin building a strategic framework. Juxtaposing these two data sets produces a matrix from which the nature and scope of the battlefield begins to emerge (fig. 4.7).

	Leaders Government	**System Essentials** Critical nodes of energy distribution, telecommunications systems, finance	**Infrastructure** Transportation, key production	**Population** Citizens	**Defense Mechanism** Military forces, law enforcement agencies
Destruction Physical destruction	Conventional weapons				
Corruption Internal operating logic	Viruses of all types, high energy radio frequency guns, ElectroMagnetic Pulse Transformer bombs, filters, agents				
Perception Management Behavior	Spamming, spoofing, misinformation, discourse, arguments, slogans, information overload				

Figure 4.7. A Basic Information-Age Strategic Framework

The Framework Shows the Existence of New Strategic Options in the Information Age

The extension of warfare to the information dimension and the permeability of that dimension presents strategic planners with options not presently available. Information technology now provides additional methodologies to isolate enemy decision makers from their own forces and populations by corrupting or denying use of their command, control, and communications systems. Manipulation of popular perceptions also offers the opportunity to force enemy leadership into situations where it must divert from a confrontational course of action or face significant opposition or severe civil unrest within its own borders.

Comparing the relationships between national centers of gravity and weapons classes also helps the strategist visualize the total battlefield and weigh available options between the use of conventional versus information weapons. For example, some weapons are likely to be more effective than others against particular enemy centers of gravity. How much more effective, of course, depends upon the capabilities of the particular weapons systems at any given time relative to the alternatives.

Ignoring a Target Is Also an Option

Not attacking a specific center of gravity or a "subsystem" within it is also a possibility that the strategic planner should not ignore. Indeed the addition of information technologies to warfare has simultaneously increased our understanding of an enemy's critical systems and at the same time provided more weapons with which to strike them. These capabilities enhance effectiveness by enabling war planners to attack critical enemy targets while allowing less critical others to be ignored. Thus *ignore* should be added to any matrix attempting to depict a relationship between weapons and targets.

Using the Basic Framework to Create Target Options

The basic strategic framework is adaptable and enables the strategic planner to quickly visualize options for implementing grand strategy. To illustrate, let us modify our strategic framework slightly to create a target matrix. Such a matrix, initially at least, would probably look something like figure 4.8. The significance of using the strategic framework in this manner is that it assists the strategist in crafting appropriate responses to different situations.

	Leaders Government	**System Essentials** Critical nodes of energy distribution, telecommunications systems, finance	**Infrastructure** Transportation, key production	**Population** Citizens	**Defense Mechanism** Military forces, law enforcement agencies
Destruction Physical destruction	X	X	X		X
Corruption Internal operating logic	X	X	X	X	X
Perception Management Behavior	X			X	X
Ignore	X	X	X	X	X

Figure 4.8. Comparing the Relationships between National Centers of Gravity and Weapons Categories Helps Visualize the Battlefield and Weigh Available Options between the Use of Conventional or Information Weapons

Take an enemy population as an example of how the target matrix might be used. In any conflict an enemy population is a difficult target to attack with traditional weapons. There are simply too many targets, and a population, particularly in an authoritarian state, is likely to suffer grievously without effect on the country's decision makers.[16] There is the additional argument that massive strikes against a civilian population may actually stiffen its will to

resist the enemy. These considerations and the theories of air proponent Giulio Douhet aside, moral objections by the American people would likely preclude the United States from launching massive conventional attacks against a foreign population.

However, while physical destruction of an enemy population is an unlikely option, the framework suggests alternative methods for breaking its morale. Information weapons capable of corrupting or denying the use of information systems that drive the machines providing essential services to the enemy population (i.e., electrical, fuel or food distribution systems, public transportation, or private financial transactions) may provide an option for the strategic planner. Such weapons, by causing severe disruption to the target population, may well generate sufficient internal pressures to force changes in an enemy's policy or leadership. In addition, efforts to manage the target population's perception of what is happening and why may be an effective or complementary strategy option.

Using the Framework to Create a Weapons-Effects Matrix

Modifying the strategic framework with weapons effects produces an effects matrix as shown in figure 4.9.

	Leaders Government	**System Essentials** Critical nodes of energy distribution, telecommunications systems, finance	**Infrastructure** Transportation, key production	**Population** Citizens	**Defense Mechanism** Military forces, law enforcement agencies
Destruction Physical destruction	-Elimination or isolation of leadership -Slows decision making	-Denial of service -Ripple effects -Isolates	-Creation of bottlenecks -Inhibits concentration of forces -Isolates	-Demoralizes -Loss of will to fight -Stiffens resistance	-Disarms -Uncovers other centers of gravity
Corruption Internal operating logic	-Produces unwise decisions -Loss of popular confidence -Isolation -Misperception of events	-Interruption/denial of service -Loss of confidence	-Creates bottlenecks -Inhibits concentration of forces -Isolation	-Creates confusion -Loss of security -Diverts energy -Promotes anxiety	-Produces unwise decisions -Isolation of leaders -Misperception of events -Failure of weapons
Perception Management Behavior	-Produces favorable decisions			-Produces pressures/ demands on leaders -Creates divisions -Manipulates passions	-Misperception of events -Produces unwise decisions -Creates divisions
Ignore	-Deemphasize damage	-Hide extent of damage	-Minor or inconsequential damage	-Control panic -Perception management	-Protect intelligence sources

Figure 4.9. A Weapons-Effects Matrix for the Strategic Battlefield

The purpose of this exercise is not to suggest that the effects noted in the matrix will always occur but to show the framework as a tool with which strategists can begin to think about the use of weapons systems and their strategic implications *and how these same concepts can be used against the United States, in the commercial, government, and military sectors of the strategic centers of gravity.*

Notes

1. John A. Warden III, "The Enemy as a System," *Airpower Journal,* Spring 1995, 47.
2. Ibid., 43.
3. Ibid., 46.
4. Ibid., 51.
5. Department of Defense, Joint Publication 3-0, *Doctrine for Joint Operations* (Washington, D.C.: The Joint Staff, 1 February 1995), GL-3.
6. Martin C. Libicki, *The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon* (Washington, D.C.: Institute for National Strategic Studies, National Defense University, McNair Paper 29, March 1994), 56–57.
7. R. Garigue, "Information Warfare: Developing a Conceptual Framework," draft discussion paper, version 2.0 (Ottawa: Office of the Assistant Deputy Minister, Defense Information Services, 23 August 1995), 32.
8. *Cornerstones of Information Warfare* (Washington, D.C.: Department of the Air Force, 1995), 4.
9. Libicki, 57; Garigue, 33.
10. Chipping is the modification, alteration, design, or use of integrated circuits for purposes other than those originally intended by the designers. It can also be a chip that is meant to fail, or to act differently than it is supposed to. Winn Schwartau, *Information Warfare: Chaos on the Electronic Super Highway* (New York: Thunder's Mouth Press, 1994), 164.

Sniffers are software programs designed to analyze a communications network. They diagnose problems and assist network administrators in fixing them. In some cases, the software is written so that network administrators are unaware someone else is snooping through their networks collecting information, such as passwords, tapping databases, and listening in on telecommunications transmissions. Sniffers may be written to ferret out information which will permit the user to surreptitiously enter and/or manipulate the system later on. Schwartau, 116.

A high energy radio frequency (HERF) gun is a radio transmitter-like device that shoots a high powered radio signal at an electronic target sufficient to disable it at least temporarily. HERF guns work by overloading the target's internal electronic circuits. Schwartau, 178–79.

The EMP/T is a nonnuclear, electromagnetic warhead that produces powerful, electromagnetic radiation. The resulting electric and magnetic fields overload and destroy electrical and electronic systems within the range of the weapon. The signals are sufficiently strong to disable any computer in their path permanently as well as destroy any floppy diskettes, hard disks, tapes, and backup tapes nearby. Schwartau, 180–81.

11. Garigue, 34.
12. Libicki, 58; Garigue, 34.
13. Garigue, 35.
14. Carl H. Builder, "Rethinking National Security and the Role of the Military," unpublished article (Santa Monica, Calif.: RAND, 6 September 1995), 14.
15. Ibid., 10. The Soviet experience suggests that totalitarian governments cannot embrace information technology and maintain a closed society. Thus information technology represents a threat to both open and closed societies for different reasons. The more open a society, the more information technology will be used and dependence upon it will grow. The higher the dependence the greater the vulnerability to information attacks. The more totalitarian the society the more information technology must be resisted. As information technology is embraced, maintaining internal control of information becomes more difficult and the society grows more vulnerable to democracy.
16. Warden, 50.

Chapter 5

Using the Framework to Analyze Information Conflicts

As stated in chapter 2, the object of grand strategy according to Clausewitz is to compel the enemy to fulfill our will by defeating his military component. In the present Information Age, the target of an attack has changed from the military to the body politic.

Primary Target in Clausewitzian Grand Strategy Changes from the Military to the People

The most effective grand strategy for offensive campaigns against an information-age society is one that focuses on destabilizing the Clausewitzian trinity by attacking the "people" rather than the "military." Information-age governments are especially susceptible not only to perception management weapons but also to public pressure generated by corruption and destruction weapons.

As previously noted, examples of information system failures caused by malevolent actors are continuing to mount. If such disruptions are occurring, it is both reasonable and prudent to assume that malevolent actors will eventually attempt to exploit vulnerabilities in unprotected information systems to achieve political objectives through a structured information attack. This is the assumption underlying the RAND war game. It is supported by the findings of a Defense Science Board report that describes the kind of threat the United States is likely to face in future conflicts.[1]

System essentials category targets like electrical power and telecommunication public switch networks have been repeatedly highlighted as susceptible to attack. The Congressional Office of Technology Assessment (OTA) wrote that US electrical systems are "vulnerable to terrorist attacks." Although no attacks have ever caused widespread blackouts, the OTA concluded "there are reasons for concern that the situation may worsen."[2] Its report cites examples of significant hostile power system disruptions in Latin America, Africa, and Europe. Likewise, a National Communications System report, issued in January 1996, voiced even more concern about the vulnerability of US public switch networks.

> The last NSIE [National Security Intelligence Estimate] risk assessment in 1993 concluded that the risk to the Public Switch Network (PSN) from electronic intrusions was a serious concern. The NSIE representatives believe that in 1995 the overall risk to the PN [sic] from electronic intrusions is greater than that reported in the 1993 risk assessment, on the basis that threats are outpacing our deterrents while vulnerabilities are outpacing the implementation of protection measures.[3]

Energy provided through natural gas pipelines has also become telecommunications dependent. Federal regulations have dictated a national standard to maintain the crucial linepack* pressure balance throughout the nation's pipelines. Federally designed "electronic bulletin boards" manage a daily balance between what local delivery companies take out of the pipelines and what suppliers put in the lines. The Federal Energy Regulatory Commission chair, Elizabeth Moler, has said the electronic bulletin boards are key in providing "both an early alert to changing conditions and a channel for instantaneous communication throughout an emergency."[4] This coordination capability, used in both daily operations and emergencies, would be lost without telecommunications system support.

The technical capabilities required to produce the incidents used in the RAND "Day After" exercise already exist. Figure 5.1 provides examples of similar real-world events for each war-game incident. The actual incidents listed below demonstrate the credibility of the RAND assumption. Each incident is more fully described in appendix B.

Applying the framework built in chapter 4 to the RAND game shows that the enemy made a concerted effort to attack the information systems that control the US system essentials. These are services, telecommunications, and banking, vital to the nation's survival and upon which millions of Americans depend. The purpose of these attacks was to produce secondary impacts upon the US population, grossly disproportionate to the actual physical damage inflicted, and thereby create pressures on US leaders to alter their chosen course.

Three-Step Framework Methodology

A methodology for applying the framework consists of three steps which are

- identify information attacks by weapons category,
- portray those attacks against the nation's strategic centers of gravity, and
- develop a weapons-effects matrix.

Application of the framework to the RAND war game, "The Day After . . . in Cyberspace," provides a good example of how the framework may be used.

Identifying Weapons Categories and Strategic Centers of Gravity in the RAND War Game

Figure 5.2 lists 23 separate information conflict incidents that occurred during the "crisis" phase of the RAND war game.** They illustrate the types of information attacks predicted by the Defense Science Board and are useful in demonstrating how to use the framework. For each example, the weapons category and target center of gravity has been identified. Examples of destructive attacks using conventional weapons have been deliberately omitted.

---

* Linepack is the amount of gas maintained in the pipeline system. Lower tolerances are established to ensure delivery capacity; higher tolerances are set to prevent safety compromises.

** See appendix B for description of the 28 incidents occurring during the "crisis" period of the RAND exercise.

Incident Number	Type of Attack	Similar World Event
3. Cairo Power Outage	Logic Bomb	Computer Espionage
4. California and Oregon Public Switch Network Shutdown	Trap Door	Legion of Doom Time Bomb
5. Ft. Lewis Mass Dialing Attack	Info Overload	Noted Intruder Skills
6. ARAMCO Explosion	Logic Bomb	Kevin Poulsen Pleads Guilty
8. Metroliner Crash	Logic Bomb	1995 Arizona Railway Incident
10. Bank of England	Sniffers	Citibank $10 Million Fraud Case
14. Time-Phase Force Deployment List Pollution	Virus	Paid Informants
15. Bank Automated Teller Machines Malfunction	Logic Bomb	$70 Million Software Glitch
19. Airplane Crash	Logic Bomb	Disgruntled Defense Contractor Employee
20. Saudi News Takeover	Spamming	Demonstrated Technology
21. Saudi Public Switch Network Shutdown	Logic Bomb	Kevin Poulsen Pleads Guilty
23. Information Warfare Attacks Against US Bases	Multiple Efforts	Defense Information Systems Agency Red Team Results
25. Joint Surveillance, Target Attack Radar System Malfunction	Worm	Electronic Intruders
26. D.C./Baltimore Phone Shutdown	Logic Bomb	Other Phone System Failures
27. Chicago Exchange Fluctuations	Logic Bomb	Shutdown Operations
28. CBS News Takeover	Spoofing	Demonstrated Technology

Figure 5.1. RAND War Game Incident Comparison

Decision makers must use personal judgment when determining appropriate centers of gravity classification for particular targets; this is especially true in the case of system essentials. Some systems, for example, telecommunications, might be part of the system essentials for more developed countries such as the United States, while for others they might not.

Using the Framework to Analyze the Enemy's Information Targets

Having identified categories of weapons and centers of gravity, placing them within the context of the basic framework enables one to begin an analysis of the attacks. Patterns begin to appear from which the outlines of the conflict begin to emerge (fig. 5.3).

Incident Number	Type of Attack	Weapons Category	Target Center of Gravity
3. Cairo Power Outage	Logic Bomb	Corruption	System Essentials
4. California/Oregon Public Switch Network (PSN) Shutdown	Trap Door	Corruption	System Essentials
5. Ft. Lewis Mass Dialing Attack	Info Overload	Corruption	Defense Mechanism
6. ARAMCO Explosion	Logic Bomb	Corruption	System Essentials
8. Metroliner Crash	Logic Bomb	Corruption	Infrastructure
9. Iranian Ambassador Statement	Discourse	Perception Management	Leaders
10. Bank of England	Sniffers	Corruption	System Essentials
11. Cable News Network (CNN) "Financial Targets" Report	Persuasion	Perception Management	Population
12. Consortium for Planetary Peace (CPP) Press Release	Slogans	Perception Management	Population
14. Time-Phase Force Deployment List (TPFDL) Pollution	Virus	Corruption	Defense Mechanism
15. Bank Automated Teller Machines Malfunction	Logic Bomb	Corruption	System Essentials
16. CNN Government Coverup Report	Persuasion	Perception Management	Population
18. CPP Demonstration	Slogans	Perception Management	Leaders
19. Airplane Crash	Logic Bomb	Corruption	Infrastructure
20. Saudi News Takeover	Spamming	Perception Management	Population
21. Saudi PSN Shutdown	Logic Bomb	Corruption	System Essentials
22. Saudi TV Announces Coup	Misinformation	Perception Management	Population
23. Information Warfare Attacks Against US Bases	Multiple Efforts	Corruption	Defense Mechanism
24. CPP News Conference	Argument	Perception Management	Population
25. Joint Surveillance, Target Attack Radar System Malfunction	Worm	Corruption	Defense Mechanism
26. D.C./Baltimore Phone Shutdown	Logic Bomb	Corruption	System Essentials
27. Chicago Exchange Fluctuations	Logic Bomb	Corruption	System Essentials
28. CBS News Takeover	Spoofing	Perception Management	Population

Figure 5.2. Illustrative Incidents from RAND War Game "The Day After . . . in Cyberspace"

	Leaders	System Essentials	Infrastructure	Population	Defense Mechanism
Destruction Physical destruction					
Corruption Internal operating logic		3 Cairo Power 4 California/Oregon Public Switch Networks (PSN) 6 ARAMCO 10 Bank of England 15 Automated Teller Machines 21 Saudi PSNs 26 D.C./Baltimore Public Switch Network 27 Chicago Trade	8 Metroliner 19 Airplane		5 Ft. Lewis 14 Time-Phase Force Deployment List (TPFDL) 23 Information Warfare Attacks 25 Joint Surveillance, Target Attack Radar System
Perception Management Behavior	9 Iran Ambassador 18 Consortium for Planetary Peace (CPP) Demo			11 Cable News Network (CNN) Report 12 CPP Press Release 16 CNN Report 20 Saudi News 22 Saudi Coup 24 CPP News 28 CBS News	
Ignore					

Figure 5.3. Illustrative Information Incidents Placed in Framework

From the representative attacks that appear in the framework, it appears the enemy in the RAND scenario has targeted the majority of its corruption weapons at the information systems controlling system essentials.* These are most likely civilian-owned and controlled systems and hence may not have the greater measure of protection likely to exist within the defense establishment. Added to this vulnerability is the fact that these systems, by definition, control essential services upon which untold numbers of the population depend. The effects of successful attacks upon them reverberate far beyond the mere shutdown of the individual systems.

* This initial impression taken from representative samples of the information incidents, such as one might expect during the initial stages of a conflict, is confirmed by a post-conflict analysis of all information incidents in the context of the framework. See appendix B.

Using the Framework to Analyze Weapons Effects

The next step in applying the framework is to develop a weapons-effects matrix that is helpful in developing grand strategy in the Information Age. Using the framework to identify target centers of gravity moves the analysis into the sphere of grand strategy. Since the object of warfare is to compel human beings to submit to the will of other human beings, identifying the people most likely to be affected by these weapons provides an important indicator of how an enemy might pursue its grand strategy.

At the strategic level, the employment of all weapons of war have purposes beyond the immediate impact of the weapon itself. For example, bombs dropped to destroy a bridge not only have the purpose of destroying the bridge but also of disrupting the transportation stream that uses the bridge. The same is true of information weapons. Hence, at the strategic level information weapons, like conventional ones, are likely to produce effects on more than one center of gravity.

Figure 5.4 shows the centers of gravity upon which the effects of our illustrative examples will land. Using the framework to identify weapons effects immediately underscores the ramifications of information conflict for the nation's leaders.

Secondary Impact of Information Attacks on Population Produces Pressure on Leaders

Attacks upon information systems that successfully disrupt services to the population produce public pressures upon political leaders to act. Perception management and corruption weapons can combine to cause significant disruptions of normal daily activities, which, in turn, generate

- public anger over the government's inability to provide protection against such weapons,
- public anxiety about the potential consequences of demonstrated vulnerabilities, and
- international questioning of US credibility.

This discontent can become a driving force to change national policies.

The fate of the American hostages in Iran is an example of how US public opinion can force decisions at the national level. As the weeks dragged by with no resolution of the Americans being held at the US Embassy in Tehran, public pressure within the United States began to mount for President Carter's administration to take some action. One result of this pressure was the decision to launch the hostage rescue attempt that ended in disaster and the loss of American life at Desert One.[5]

A hypothetical incident in the RAND war game illustrates the point. As an ally of the United States, Great Britain is also the subject of information attacks. The Bank of England discovers the presence of "sniffers" in its electronic funds transfer system. Immediate ramifications are that Britain suspects it is under attack because of its alliance with the United States. CNN broadcasts a report of the attack (incident 11) that produces an immediate 10 percent drop in the stock market because institutional investors move to get out of the electronically managed market. The Security and

	Leaders	System Essentials	Infrastructure	Population	Defense Mechanism
Destruction Physical destruction		6 ARAMCO	8 Metroliner 19 Airplane	8 Metroliner 19 Airplane	
Corruption Internal operating logic		3 Cairo Power 4 California/Oregon Public Switch Networks (PSN) 5 Ft. Lewis 6 ARAMCO 10 Bank of England 15 Automated Teller Machines (ATM) 21 Saudi PSNs 23 Information Warfare (IW) Attacks 26 D.C./Baltimore PSN 27 Chicago Trade	8 Metroliner 19 Airplane	3 Cairo Power 4 California/Oregon PSNs 15 ATMs 21 Saudi PSNs 26 D.C./Baltimore PSN 27 Chicago Trade	5 Ft. Lewis 14 Time-Phase Force Deployment List (TPFDL) 23 IW Attacks 25 Joint Surveillance, Target Attack Radar System (JSTARS)
Perception Management Behavior	3 Cairo Power 4 California/Oregon PSNs 5 Ft. Lewis 6 ARAMCO 8 Metroliner 9 Iran Ambassador 10 Bank of England 11 Cable News Network (CNN) Report 12 Consortium for Planetary Peace (CPP) Press Release 14 TPFDL 15 ATMs 16 CNN Report 18 CPP Demo 19 Airplane 20 Saudi News 21 Saudi PSNs 22 Saudi Coup 23 IW Attacks 24 CPP News 26 D.C./Baltimore PSN 27 Chicago Trade 28 CBS News			8 Metroliner 10 Bank of England 11 CNN Report 12 CPP Press Release 15 ATMs 16 CNN Report 19 Airplane 20 Saudi News 21 Saudi PSNs 22 Saudi Coup 24 CPP News 26 D.C./Baltimore PSN 27 Chicago Trade 28 CBS News	5 Ft. Lewis 14 TPFDL 23 IW Attacks 25 JSTARS
Ignore					

Figure 5.4. Using the Framework to Identify Where the Effects of Information Weapons Fall

Exchange Commission reports a "pattern of institutional investment manipulation." Public anxiety and anger concerning the integrity of the nation's financial system mount, giving rise to a major perception management problem for US political leaders. In information warfare, the secondary effects are likely to be more important than an attack's immediate damage.

Perception Management Is the Common Thread in Information Conflicts

From a government leadership perspective, the majority of information-age weapons land with at least one foot in the perception management category. Corruption or destruction weapon types are normally targeted against organic essential or infrastructure centers of gravity but clearly their effects are not limited to these categories. Perception management issues are particularly critical for leaders because they must be able to address the people's anxieties and concerns. Information attacks will generate such questions from the public as:

- What other systems are vulnerable?
- How big is this problem?
- Why has the government not provided greater security?
- Who is responsible for defending against these attacks?
- What are they doing about it?

Information-age media compounds the problem. Consider, for example, public reaction to the president or telecommunications chief executive officers after a public switch network, which serves as a transfer point for thousands of communications each day, fails for a third time. When answers remain scarce, public support for senior leadership is sure to wane. The degree of skill demonstrated in handling these issues determines the ability of government leadership to maintain the fragile link between Clausewitz's government leadership and their people. Unless leaders can answer the people's questions satisfactorily, the danger exists that public pressure will force national security policy changes that may not be in the nation's best interest.

Notes

1. Department of Defense, *1994 Defense Science Board Summer Study on Information Architecture for the Battlefield* (Washington, D.C.: Defense Science Board, 1994), 28 and 51.

2. Congress and Senate, Office of Technology Assessment, *Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage* (Washington, D.C.: Government Printing Office, June 1990), 1–2.

3. United States, National Communication System, *An Assessment of the Risk to the Security of Public Networks* (Washington, D.C.: National Communications System, December 1995), ES-1.

4. International Energy Agency, *The International Energy Agency Natural Gas Security Study* (Paris: Organization for Economic Cooperation and Development/International Energy Agency, 1995), 183.

5. Warren Christopher et al., *American Hostages in Iran: The Conduct of a Crisis* (New Haven: Yale University Press, 1985), 180.

Chapter 6

Conclusions

The emerging Information Age has brought enormous benefit to the United States. US technological superiority promises to maintain the nation's world leadership well into the next century. However, US reliance upon technology has grown into dependence, and that has resulted in a new form of strategic threat aimed at the information systems that control key aspects of its military, economic, and political power.[1] This new strategic threat calls for a rethinking of US grand strategy for Information Age national security.

Rethinking Grand Strategy Requires Vision and Public Debate

Such an effort requires us to rethink our basic national security objectives. We must start with the most important question: What do we want to achieve? In the United States, the answer to that question requires both vision and national debate. The vision that is beginning to emerge is information assurance. Simply put, we seek to promote the confidentiality, integrity, and availability of our information and the reliability of our information systems. However, it is a vision that, given the present state of technology, does not permit universal attainment. The US government alone cannot provide security for the entire information spectrum nor for the interconnected systems that run the nation's critical assets. Therefore, we must abandon the idea of universal protection in favor of selective defense. We must focus on those systems deemed essential to the nation's health.

The impossibility of providing universal protection requires the setting of priorities that in turn require an assessment of information's value and its vulnerabilities. These requirements give rise to public debate. Given the pluralistic nature of our society, the equities of competing interests in the information infrastructure and the pervasiveness of information technology, the debate is likely to be lengthy and vigorous. The Department of Defense, as the nation's principal defender, can and should play a leading role in this discussion, but it cannot dictate the outcome. The problem is national in character and the debate must push past government and military discussions until a public consensus that balances the need for government security and personal protection with US constitutional guarantees and American notions of individual liberty emerges.

A Theme for US Defensive Grand Strategy

The strategic framework we have constructed suggests information assurance should be the theme for US defensive grand strategy. The protection of the information and

information systems that are critical to US strategic centers of gravity against destruction, corruption, and perception management weapons must become the catalyst for cooperation between government and civilian entities and the driving force behind the development of new national security policies. Just as "containment" unified national policies and provided a framework for meeting the Soviet strategic threat, so must information assurance provide the basis for a unified response to meet the strategic information threat.

A Pluralistic Framework for the Exercise of Power Is Needed

The hard nut to crack in an information-age democracy is defining a legitimate role for government that promotes the nation's security while protecting its constitutional guarantees and individual liberties. The purpose of our constitution is "to provide for the common defense, promote the general welfare and secure the blessings of liberty to ourselves and our posterity." The genius of the American political system is that it has based its institutions firmly on the concept of division of authority and separation of powers. No one governmental entity has been permitted to amass power to the exclusion of other governmental entities that may reflect different points of view or represent other constituencies. In the final analysis, we are a nation that relies upon the principle of shared authority to keep the exercise of governmental power in balance among divergent and sometimes competing interests. Given the pervasiveness of information technology and its importance throughout the political, military, economic, and social fabric of American life, proposals to defend against the information threat by abandoning this principle of shared authority in favor of concentrating power will likely meet overwhelming opposition from the body politic. The nation is not, however, without experience in creating frameworks that recognize differing viewpoints and different constituencies while exercising legitimate governmental powers in furtherance of national security.

Executive Orders 12656, 12919, 12148, and 12472 comprise the legal basis for preparation of national security emergency preparedness plans, the purpose of which are to ensure the continuity of government at every level in the event of a national security emergency.[2] A product of the nuclear age, these orders instruct in general terms various designated executive department heads to identify functions within their areas of respective interest that would have to be performed during national emergencies and to develop the plans and capabilities to do so. They are a formula for protection of the nation's most critical assets in the event of a national crisis. The secretary of agriculture, for example, plans for resources preparedness with respect to food resources and food resource facilities; the secretary of energy does the same with respect to all forms of energy; the secretary of health and human services looks after the nation's health resources, and so on.[3] These are useful precedents in planning to defend against the information threat because they demonstrate how to divide and allocate authority and resources among various agencies representing different constituencies and different sectors of the economy in furtherance of national security.

The challenge of the information strategic threat is a national challenge. The military alone cannot defend against it. Arguably, neither can any other single entity of national government. What is needed is a national entity, a National Information Assurance Council (NIAC), chaired by the vice president and composed of permanent representatives from each executive department agency that attends to a portion of the civilian infrastructure deemed vital to national security. The council's charter must be strategic in scope and focus on presenting to the president national policy recommendations aimed at bringing about a vision of information assurance based upon the confidentiality, integrity, availability, and reliability of our information and information systems. It must be able to allocate finite resources, assess risks, fix responsibility, and perform emergency preparedness planning to promote information assurance. Its members must be free to focus on *national* information assurance matters while at the same time representing their respective constituencies in the process of policy formulation. Since hostile competitors will most likely attack those critical private sector system essentials whose destruction or damage will cause the greatest disruption among the civilian population, the council must recognize that defensive information warfare encompasses a much broader spectrum of activities than just protecting friendly command and control systems or vital industrial resources from the threat of hostile information attacks. To be effective, its defensive planning must include measures to defend high-value, private sector information and information systems. The council must be linked to the president's National Security Telecommunications Advisory Committee (NSTAC) and to other similar committees representing priority areas for protection. This linkage will help ensure that private sector concerns are brought to the table. In addition, the presence of representatives from the agencies representing these constituencies will help guarantee that private sector commercial needs are not subsumed by the quest for ever greater security.

A Single Agency Executive Agent for Information Assurance Is Contraindicated

The nature of conflict has not changed. Warfare's purpose continues to be the coercion of an adversary "to fulfill our will."[4] In this respect, warfare in the Information Age promises to be no different.[5]

The Department of Defense is charged with defending the nation and should play a leading role in the discussions concerning how to defend in the information dimension of warfare. It has developed the planning expertise, institutions, and human resources to do so. The appearance of new methods and concepts that competitors might seek to attack targets within the United States does not transform conflict in the information dimension into something other than strategic warfare. Its characteristics remain the same: in this case, to force US compliance with a hostile competitor's objectives.

DOD, however, has neither the organizational breadth nor the jurisdictional authority to serve as the lead agency in formulating grand strategy to defend the United States against the information threat. At present, the military services are focusing on their respective pieces of "information dominance." These efforts represent a wartime subset of

an information assurance national security grand strategy. While they are important, they are only a part of the total information assurance needed, and no matter how well they are developed, they will fall short of a national defense because they do not protect vulnerable information assets in the civilian infrastructure upon which DOD relies.

Neither is the Department of Justice an appropriate lead executive agency as some have advocated. To place responsibility for the nation's defense against the information threat into the hands of the Justice Department commits that responsibility to an organization with limited institutional and historical skills in national defense planning. Furthermore, the Justice Department has comparatively limited jurisdiction and experience in worldwide operations and limited capability to respond externally to structured threats. In addition, as an agency engaged in domestic law enforcement activity, the Justice Department faces a built-in conflict of interest whenever national defense precautions include the official monitoring of private sector security practices and confidential information. This is an important, perhaps crucial, consideration in winning private sector support for national information assurance policies.

Priorities for Protection within US Strategic Centers of Gravity

Our strategic framework suggests the United States must prepare itself to defend both private sector and government information systems. Universal protection is not attainable, nor do we believe it is necessary. A large majority of the material within the information hierarchy of available data, information, knowledge, and wisdom is not vital to national security. Likewise, not all of the hardware that forms information systems and networks that make up the civilian information infrastructure requires protection. In each case, only a small portion of the total amount of information available or number of information systems in operation must be secured against external forces that would seek to manipulate them. In the case of information itself, the existing paradigm seeks to protect official US government classified information. That model is clearly outdated and must be revised to include, at a minimum, information that runs sectors of the economy we have labeled system essentials (fig. 6.1). With respect to information systems, more and more attention is being paid to the vulnerability of the Public Switched Network (PSN), the critical nodes within the telecommunications industry that route message traffic. Clearly the PSNs must be placed high on any list of information systems to be guarded against tampering.

We have categorized as system essentials information and information hardware that control the nation's strategic centers of gravity. These system essentials offer the most lucrative information targets for competitors as their disruption may cause massive unrest among the civilian population and, thereby, generate significant political pressures upon the nation's political leaders. We believe priority must be given to these for protection. In addition, within the strategic centers associated with government, that is, leaders and the defense mechanism, those systems that permit command and control and employment of military forces must also be protected. We believe the balance of information and information systems should be left to the private and commercial sectors.

Leaders	System Essentials	Infrastructure	Population	Defense Mechanism
Command and Control Networks	Telecommunications Electric power Gas/oil pipelines Federal Inter-bank transfers	Transportation dispatch systems		Communications networks Logistics/Personnel databases Transportation management systems

Figure 6.1. Priorities for Protection

Defending against Physical Destruction of Information Systems

Executive Order 12656, that assigns certain National Security Emergency Response Preparedness (NSERP) activities to the Department of Defense, specifically identifies technological emergencies as an example of a national security crisis requiring DOD's response. Section 204 requires the secretary of defense to:

> Identify facilities and resources, both government and private, essential to the national defense and national welfare, and assess their vulnerabilities and develop strategies, plans, and programs to provide for the security of such facilities and resources, and to avoid or minimize disruptions of essential services during any national security emergency.[6]

Originally designed to ensure the continuity of government in the event of a nuclear war, section 204 nevertheless provides the legal basis for the secretary of defense to begin planning for the protection of critical US public and private information systems from physical attack. DOD's NSERP planning should be modified to provide physical protection not only for industrial facilities and resources that are deemed critical to the mobilization and employment of military forces but also for key network switching and control systems that manage areas within our strategic centers of gravity designated for priority protection (fig. 6.1). Nomination of such areas from outside DOD should be made by representatives on the National Information Advisory Council.

Defending against Corruption of Information Systems

The threat to US information systems from corruption weapons is a clear and present danger that demands immediate attention. Unfortunately, it is also a threat that requires long-term as well as short-term solutions. Long-term solutions require the establishment of national institutions with broad charters that cross traditional bureaucratic boundaries, such as NIAC, and vigorous national debate concerning the proper measure of government involvement in something as pervasive in American life as information management. Short-term solutions are primarily within DOD and should be pursued immediately.

Both the government and the private sector have had experience with taxonomies that are useful in fashioning separate but complementary responses to the information threat. With respect to the government, institutions existing within the public health sector, particularly the Center for Disease Control, appear to be applicable. In the private sector, national testing organizations such as the National Underwriter's Laboratory provide useful designs for reference.

Use of the term *virus* for software programs that surreptitiously enter computers and attack their internal operating systems is an apt metaphor. The characteristics of information conflict, in many respects, are very similar to those of infectious diseases. Anyone or anything can be an infectious disease carrier. New disease strains can circumvent or overcome prepared defenses. Disease carriers are hard to trace, and infectious diseases can pass through multiple carriers. The same is true of information conflicts.[7]

Just as it took the federal government to marshal the resources and expertise necessary to mount an effective counterattack against the spread of infectious diseases, so should the federal government create the national institutions and processes necessary to blunt and roll back the onslaught of electronic diseases. As we have seen, the spread of electronic infections through networked technology places the nation's well-being clearly at risk. As the entity responsible for information assurance, NIAC should establish a separate information assurance center patterned after the Center for Disease Control to combat the strategic threat posed by the outbreak of electronic epidemics.[8]

NIAC's information assurance center should be resourced and empowered to carry out four functions: surveillance, research, prevention, and control and infrastructure (fig. 6.2).[9]

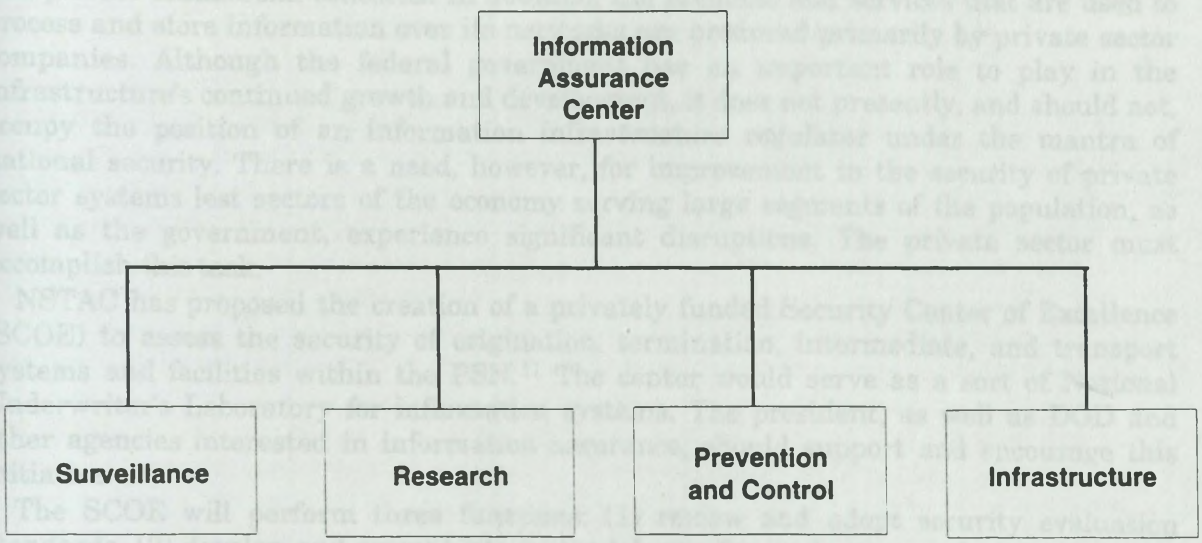


Figure 6.2. Information Assurance Center

The surveillance function should monitor the outbreak of electronic infections both within the United States and internationally. The history of public health teaches that suppression of infectious diseases must be preceded by an understanding of their behavior and the methods of their transmission.[10] The same is equally true of information corruption weapons. Within the United States, reporting criteria must be implemented to ensure that the new information assurance center is properly notified of potentially contagious, electronically induced disruptions of service within designated priority areas for protection and/or of the employment of certain types of information corruption weapons.

Research should focus on how hardware, software, and human behavioral factors influence the emergence or prevention of information corruption; the effectiveness and economic benefit of strategies to prevent corruption of information systems; and the development of improved techniques for identifying emerging technologies that promote or restrict the spread of electronic infections. An added function is to establish programs to promote effective partnerships with public agencies, universities, and private industry to support research in surveillance, and the prevention and control of technological attacks against information systems.

Prevention and control deals with public education and the implementation of measures designed to prevent or contain the outbreak of infectious information attacks. This function includes the development and dissemination to the public information that informs and educates about the nature, methods of transmission, and pathologies of information corruption software. It also contains rapid-response teams to investigate and contain massive disruptions of systems that control priority areas for protection.

The infrastructure function looks to development of a national network of professional and support personnel to understand, monitor, and control electronic infections. It will provide training in reporting criteria, diagnostic evaluation, and surveillance of new and reemerging threats.

National security strategists must remember that the US information infrastructure is a creature of the private sector. It is being built, owned, and operated by private citizens and private commercial concerns. In addition, the products and services that are used to process and store information over its networks are produced primarily by private sector companies. Although the federal government has an important role to play in the infrastructure's continued growth and development, it does not presently, and should not, occupy the position of an information infrastructure regulator under the mantra of national security. There is a need, however, for improvement in the security of private sector systems lest sectors of the economy serving large segments of the population, as well as the government, experience significant disruptions. The private sector must accomplish this task.

NSTAC has proposed the creation of a privately funded Security Center of Excellence (SCOE) to assess the security of origination, termination, intermediate, and transport systems and facilities within the PSN.[11] The center would serve as a sort of National Underwriter's Laboratory for information systems. The president, as well as DOD and other agencies interested in information assurance, should support and encourage this initiative.

The SCOE will perform three functions: (1) review and adopt security evaluation standards, (2) develop and promulgate methodologies for evaluating and rating security

products and systems, and (3) enhance communications between industry, government, and the public on the need for implementation of information assurance measures.[12] An entity that performs these functions in an environment free of bias and conflict of interest will serve a number of useful purposes.

First, it will provide standards and methodologies that testing laboratories can use to evaluate the security of existing products and of those being introduced into the market. Such testing, impossible in the absence of recognized industry standards, will provide a means of measuring product and system trustworthiness and integrity. The introduction of standards where none now exist will gradually produce a marketplace that generally reflects the level of security promulgated as being usual and customary within the particular industry being examined. The result is an overall improvement of security within the information infrastructure.

Second, the introduction of industry-wide security standards limits the liability of companies that adhere to them. A company that implements security measures commensurate with those recommended by the SCOE will most likely have met the reasonably prudent person standard that results in the avoidance of liability in civil litigation. The converse, of course, is that companies ignoring such standards are likely to find themselves the targets of civil lawsuits. Hence, the existence of standards performs an additional function of regulating the industry by exposing those who do not follow them to the risk of serious financial hardship and likely loss of business.

Finally, publication of security standards can be expected to help stimulate public interest in and demand for products and services that provide a greater measure of information assurance, balancing protection and privacy. NSTAC predicts that upon publication of such standards, the security consulting industry will move to promote and implement them, resulting in their rapid adoption throughout the infrastructure.[13] The end result will be a more reliable PSN.

Defending against Perception Management

"Our influence will increasingly be defined more by the quality of our ideas, values, and leadership . . . than by the predominance of our military capabilities."[14] In an age where information is instantly disseminated, ideas count as never before. Determined adversaries will use perception management techniques to manipulate ideas to push US public opinion toward positions that favor their own and to undermine public confidence in national leaders who oppose them.

Above all else, US policy makers must communicate the goals and objectives of national security policies clearly and simply. Such communication promotes understanding by the widest possible audience and helps to generate support for the commitment of US forces in furtherance of national security objectives. It also helps to ensure that the nation's security policies conform with America's declared ideals and beliefs. If otherwise, the images generated by adversaries will quickly point out the dichotomy and predispose the American population to the employment of other perception management techniques.

The importance of ideas in a era of instant communications means that the US must be capable of responding to media demands for instantaneous reactions to world events with

positive real-time images of its own in support of national policies. The government's knowledge machinery that supports the president and senior government leaders must be able to prepare both information and, more importantly, compelling television video as quickly as CNN can present its news and analysis. The objective must not be to point the television spotlight elsewhere, dim it, or switch it off but rather to challenge it for accuracy and context with images that counteract distortions and half-truths.

Determining the adequacy of these defensive countermeasures will require new measures of effectiveness for grand strategy. We presently have no definable method to assess the criticality of individual pieces of the infrastructure, or the benefits of protecting them, or the risks of not protecting them. Without these measuring tools, and the sound logic needed to produce them, the effort to build adequate defensive countermeasures will lag behind offensive capabilities.

Notes

1. Kenneth E. deGraffenreid and Michelle Van Cleave, "Information Assurance and the Future of the NCS," draft (Fairfax, Va.: National Security Research, Inc., 12 May 1995), 5–6.

2. Executive Order 12148, "Federal Emergency Management," 44, *Federal Register* 43239, 20 July 1979; Executive Order 12472, "Assignment of National Security and Emergency Preparedness Telecommunications Functions," 49, *Federal Register* 13471, 3 April 1984; Executive Order 12656, "Assignment of Emergency Preparedness Responsibilities," 53, *Federal Register* 226, 18 November 1988; Executive Order 12919, "National Defense Industrial Resources Preparedness," 59, *Federal Register* 29525, 3 June 1994.

3. Executive Order 12919, *Federal Register,* sec. 201.

4. Carl von Clausewitz, *On War,* ed. and trans. Michael Howard and Peter Paret (Princeton, N.J.: University Press, 1976), 89.

5. David S. Alberts, *Defensive Information War: Problem Formulation and Solution Approach* (Washington, D.C.: National Defense University, 17 January 1996), 5.

6. Executive Order 12656. *Federal Register,* sec. 226.

7. Paul A. Strassmann, "Defending the Military Infrastructure," address, National Defense University, Washington, D.C., 11 March 1996.

8. Paul A. Strassmann, "Risk-Free Access into the Global Information Infrastructure Via Anonymous Re-Mailers," (Symposium on the Global Information Infrastructure, Kennedy School of Government, Harvard University, 28–30 January 1996). The metaphor of infectious diseases and the concept of a Center for Disease Control-like response within DOD is the brainchild of Mr. Strassmann.

9. The functions of the proposed DOD information assurance center were adapted from *Addressing Emerging Infectious Disease Threats: A Prevention Strategy for the United States* (Atlanta, Ga.: Center for Disease Control and Prevention, April 1994).

10. Strassmann.

11. National Security Telecommunications Advisory Committee (NSTAC), *Report to NSTAC XVIII* (Washington, D.C.: National Information Infrastructure Task Force, February 1996), B-3.

12. Ibid., B-7.

13. Ibid., B-8.

14. The White House, *National Security Strategy of the United States* (Washington, D.C.: Government Printing Office, August 1991), 14.

Chapter 7

Recommendation . . . A Strategic Plan

We insure against loss of life, against loss of money, against destruction by fire or storm, and, in fact, against the loss of possession or attribute which we deem of value. . . . The country or state is the highest form of insurance policy, and it is underwritten by a policy of national defense.

—John Weeks
Secretary of War, 1923

A Strategic Plan for National Security

Our vision provides a focus for long-term planning, and the mission establishes our day-to-day responsibilities. Mission-related decisions are made not only to accomplish short-term objectives but to achieve the vision. "Vision focused and mission driven" define our boundaries. The goals of this plan provide priorities as we move forward to achieve its vision.

The momentum of recent efforts to address the issue of information assurance positions the US to make great progress in the years ahead. However, we must keep in mind two points: *First,* it will take time, patience, and persistence to refine this plan and to develop the relationships necessary to achieve its goals. *Second,* we need to start now.

The course is set.

Vision: Information Assurance for the Twenty-first Century

- A national commitment that secures confidentiality, integrity, and availability of information and the reliability of information systems.
- A national consensus balancing government security and personal protection with US constitutional guarantees and American notions of individual liberties.

Mission: Plan, Assess, Coordinate, and Conduct Activities to Achieve Information Assurance

- Identify and assess vulnerable information nodes within priority areas for protection.
- Identify and assess the strategic threat to US information and information systems.
- Develop proactive prevention and control measures that detect, deflect, and defeat intrusions into, or structured information attacks upon, priority areas for protection.
- Develop the capability to execute those plans.
- Develop national institutions that build US government and private sector equities in information assurance.

Goals: National Imperatives

We must produce a national security grand strategy that includes defending the nation's information infrastructure, because the nation's viability—political freedom, economic identity, and military power—now depends upon it. Achieving this objective will require educating the American people to understand that national security is not the sole responsibility of the DOD and includes traditional economic, political, and military boundaries. We must seek to promote vigorous public debate about the role of government in information assurance to build a strong national consensus as to how we will achieve our goals. The debate must clearly include an assessment of the need for intelligence sharing among all the national security stakeholders. Painful choices may have to be made to reshape national defense policy in the Information Age.

- Lead a vigorous public debate. The Information Age presents security risks that are economic and political, and not solely military in nature. These threats must be made known to the American people as a first step in building public support for new national security priorities that are becoming more complicated daily. Government agencies and the commercial sector must find common ground to underwrite a national commitment to information assurance.
- Unify a government/private sector response to protect the confidentiality, integrity, availability, and reliability of US information and information systems against the strategic information threat. Replace "containment" with "information assurance" as the vision upon which US national security grand strategy is based.
- Abandon the idea of universal protection in the information dimension in favor of selective defense that focuses on both government and private sector information and information systems deemed critical to national security.
- Give information assurance priority for protection to the system essentials strategic center of gravity and, within it, specifically to telecommunications switches, electric power distribution mechanisms, gas and oil pipeline distribution mechanisms, interbank transfer mechanisms, and transportation dispatch systems. Within the defense mechanism center of gravity, communications networks, logistics and personnel databases, and transportation management systems must also be protected.
- Establish a National Information Assurance Council (NIAC) to make national security policy recommendations to the president aimed at bringing about our national security vision of information assurance.
- Establish an Information Assurance Center, patterned after the Center for Disease Control, and answerable to NIAC to perform surveillance, research, prevention and control, and infrastructure functions within the information assurance mission.
- Expand US National Security Emergency Response Preparedness (NSERP) planning to include physical protection for key network switching and control systems that manage areas within our strategic centers of gravity designated for priority protection.
- Encourage the president and Congress to support the National Security Telecommunications Advisory Council (NSTAC) efforts to establish a Security Center of Excellence and expand the NSTAC concept by creating similar committees in areas designated for priority protection.

- Enhance the president's knowledge machinery to provide timely responses to the media's demand for immediate reactions to national security events and to provide accuracy and context to media reporting.

Goals: DOD Imperatives

The US military must play a leading role in devising this strategy but cannot do it alone. DOD must be included in any strategy for defending military and commercial information systems because our national defense depends upon it, and the ability to bring combat power to bear in support of national objectives relies on its ability to deploy and sustain American forces. In the short term, DOD must act to resolve its own information assurance requirements and to understand that national security in the Information Age is more than information dominance.

- Submit information assurance and its information-age strategic implications by the Secretary of Defense as part of the next national security strategy.
- Direct chairman of the joint chiefs of staff to promulgate a new national military strategy that addresses the information assurance vision and its wartime subset of information dominance. As "containment" carried significant grand strategy meaning throughout the cold war, so a new policy of "information assurance" must be understood at the grand strategy level and as a part of the national security strategy.
- Retitle the assistant secretary of defense for C3I as the assistant secretary of defense for information. Expand the position's focus beyond C3I to incorporate such areas as continental United States (CONUS) defense against information attacks.
- Assemble a DOD organization for defense information assurance. Use core competencies already available within DOD to replicate the health taxonomy used for national information assurance. Figure 7.1 displays some possibilities.

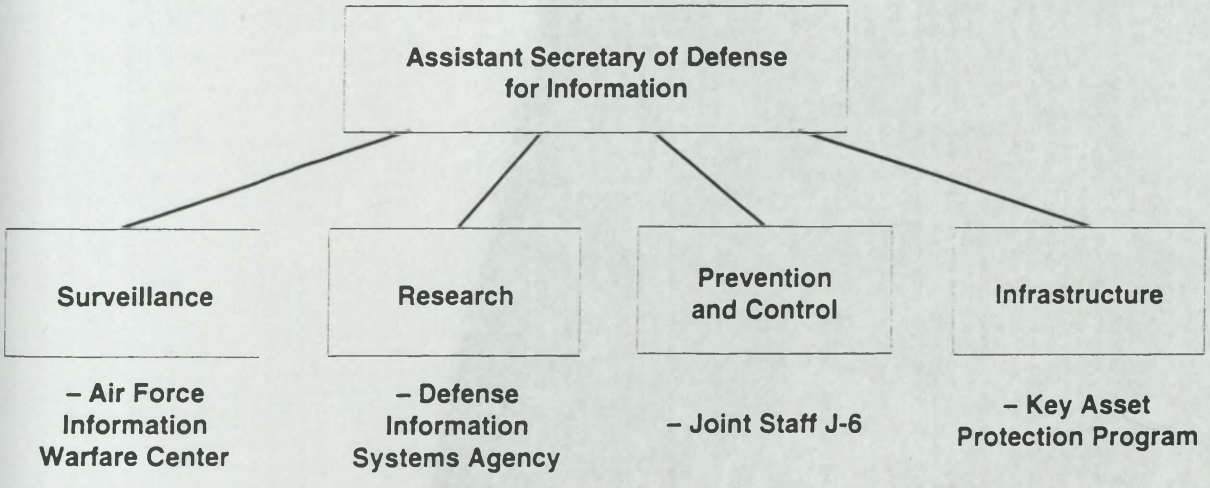


Figure 7.1. Sample Military Information Assurance Hierarchy

- Recommend a change to the Unified Command Plan. Designate CONUS as an area of responsibility (AOR), task commander in chief, United States Atlantic Command (CINCUSACOM) or commander in chief, Strategic Command (CINCSTRATCOM) with a CONUS-defensive information warfare responsibility. Include an aggressive, quantitative modeling and simulation effort for defensive information warfare.
- Direct CINCUSACOM to restructure the Key Asset Protection Program (KAPP) by: (1) assessing key asset vulnerabilities to corruption information weapons as well as physical destruction weapons; (2) adding system-essential priority areas for protection to the Key Asset List; (3) expanding the KAPP evaluation and review board to incorporate experts from appropriate fields; (4) expanding planning and training to incorporate new Key Asset List physical protection requirements; and (5) thoroughly documenting all actions needed to address information vulnerabilities.
- Merge KAPP analysis with current vulnerability net assessments to identify the potential repercussions of a structured information attack upon system-essential assets. Assume aggressive, quantitative modeling and simulation effort for defensive information warfare. Recommend higher levels of information assurance for national security.
- Direct a review of operational plans for the land defense of CONUS to incorporate potential impacts resulting from information attacks and degradations to the information infrastructure. Include aggressive modeling and simulation as part of the OPLAN review.
- Direct a review of defense contingency plans to ensure they incorporate the full breadth of information warfare options and brief the NSC on these new options as well as the potential for their use against the United States.

Appendix A

Anecdotal Evidence

The following incidents are not provided to suggest chaos on the information highway, but rather that, in the hands of malevolent actors, the capability already exists to cause significant disruption to information systems vital to US national security. While assertions of a national disaster may be somewhat premature, anecdotal evidence suggests the United States is already vulnerable to information attacks. In recent years, unknown intruders have penetrated US telecommunications carriers, Internet service providers, many international post, telegraph, and telephone entities, and a wide variety of end-user systems.

Wired magazine names the top ten infrastructure targets including the Culpeper Public Switching Network (PSN) that handles federal funds transfers and Worldwide Military Command and Control System (WWMCCS).[1] Additional targets include satellite dishes associated with the global positioning system (GPS) (and time synchronization for precision munitions); satellite dishes associated with national intelligence and defense activities (the "Big Blue Cube" in Mountain View, California, and the National Photographic Intelligence Center); the Internet; computer-directed telephone and power distribution transfer points (including the Alaskan Pipeline); and computers associated with major banking and financial institutions. Targets of intrusion include

- physical attacks on infrastructure components such as computers, communications, software, data cables, and control process; infrastructure support such as buildings, power and environmental control units; and attacks or subversion of operating and support personnel,
- logic attacks on infrastructure components; attacks on computer-controlled environmental control units; and attacks on data (destruction or corruption), and
- combined logic and physical attacks to mask each other.[2]

Financial Losses

In 1991, the FBI director said "as much as $5 billion a year" was lost by American companies due to computer-related crime.[3] By 1995, the *Dallas Morning News* reported "$10 billion worth of data" was stolen annually in the US from "on-line thieves."[4] The real threat to American interests lies in the ability of criminals to infiltrate and destroy US financial and information systems. Hackers who pioneered breaking into computer systems for fun are selling their abilities to criminals.

- The *New York Times* reported in August 1995 that a $10 million computer fraud case had been uncovered involving a 34-year-old Russian and accomplices who, from his keyboard in St. Petersburg, Russia, moved money via wire transfers from Citibank accounts in Argentina and Indonesia. In response, a bank spokesperson ensured that all but $400,000 of the cash had been recovered and offered some perspective to the

problem. She said, "We move half a trillion dollars a day through the payment system . . . compare that to $400,000 . . . we think we have the right level of security." In major bank frauds involving electronic funds transfers, first detection is normally the bank audit, usually several months after the incident.[5]

- During the Soviet era, criminal groups and the black market functioned as an extension of the Communist Party and the State Security Committee (KGB). These criminal organizations outlived the state that fostered them. There are roughly 5,700 organized crime groups in Russia. Of these, 200 are large sophisticated criminal organizations engaged in activity throughout the former Soviet Union and in 29 other countries. These criminal groups are also targeting the financial sector. Banks have become a particular target for money laundering schemes. Links have been forged between Russian and Italian organized crime groups to move money through the Russian banking system.[6]
- A software glitch was the cause of a $70 million government loss due to overpayment by the Health Care Financing Administration. About 100 health care organizations received overpayment—the largest was $19 million—due to a software problem that failed to cross-check Medicaid charges against people eligible for Medicaid.[7]
- In 1991, a US car manufacturer lost approximately $500 million when a hacker broke into its network and stole future auto designs that ended up in the hands of its competitors.[8]
- A 1994 survey of business losses due to information security problems had 1,271 respondents of which over 50 percent claimed financial losses due to information security issues; 17 percent had losses up to $250,000; 3 percent had losses between $250,000 and $1 million; and 17 percent reported losses in excess of $1 million. Biggest concern is integrity and availability of information.[9]
- In October 1992, Internal Revenue Service (IRS) internal auditors identified 368 employees who had used the IRS's Integrated Data Retrieval System without management knowledge for nonbusiness purposes. Some of these employees had used the system to issue fraudulent refunds or browse taxpayer accounts that were unrelated to their work.[10] In April 1996 a former IRS worker pleaded guilty to federal charges for illegally tapping into more than 150 confidential tax records.[11]
- Authorized users of the FBI's National Crime Information Center misused the network's information by gaining access to files to determine if friends, neighbors, or relatives had criminal records or inquire about backgrounds for political purposes.[12]
- National Communications System (NCS) says there is significant evidence of insiders' selling information to information brokers, industrial spies, criminal organizations, and intelligence services. These insiders, with full access to their respective information files, have provided data on unpublished telephone numbers, toll records, credit reports, and other personal data. The FBI reported that criminal organizations have gained access to the National Crime Information Center records primarily through the use of compromised employees. In December 1991, 18 Social Security Administration employees were indicted for sale of confidential information.[13]
- In August 1992, a computer systems administrator for a defense contractor was told of a pending layoff. The employee set up a malicious code to activate after his departure. He hoped that the company would hire him back to reconstruct databases

after the logic bomb functioned. His attempt was discovered before he left and he later pleaded guilty to the charge. If the malicious code had functioned, substantial data on the development of military missile systems would have been destroyed and required months to reprogram the computer system.[14]

Telecommunications Targets

The public telecommunications networks are a critical part of the Defense Information Infrastructure/National Information Infrastructure (DII/NII) (95 percent of DOD telecommunications is provided by public networks and operated by common carriers) but lack the assurance features needed for military use.[15] There have been multiple incidents (mostly accidental) in which the assurance designs were unable to meet the challenge of accidental errors and omissions. Most commercial networks have little or no coverage against intentional disruption and commonly fail due to software errors or mischievous or malicious attacks. Additionally, telephone switching errors must be repaired within 1.5 seconds or the circuit errors passing through the network will propagate, causing major disruption. An attacker needs to disrupt only two of the nine PSN sites for 1.5 seconds to cause a cascading effect.[16]

- In 1991, a near-total shutdown of telephone service in the Baltimore-Washington area was caused by a 3-bit coding error where a "d" was replaced by a "6" in one byte of a software upgrade, causing disruption of AT&T long distance service to millions of customers for more than four hours. None of the few broad phone outages that have occurred has been shown to be caused by anything other than faulty software, though the signaling systems have been under hacker attack affecting service to customers. The point made is that though there have been no catastrophic failures, the potential exists.[17]
- On 17 September 1991, AT&T announced a "power failure" had caused two major switches to fail. This failure forced the shutdown of major airports that rely on ground-based telephone lines for both voice and data communications for air traffic control in the New York City, Boston, and Washington air route traffic control centers. The result was disruption of the civil aviation industry into the northeast United States for days, resulting in flight delays across the nation.[18]
- In 1993, Federal Aviation Administration (FAA) computer system failures (cause unknown) delayed regional traffic for 90 minutes and an FAA weather computer failed for 12 hours due to a time-activated logic bomb.[19]
- Examples of other phone system failures include a highway crew's digging post holes causing disruption of coast-to-coast calls by cutting a MCI fiber-optic cable. A similar incident in New Jersey cut 60 percent of the calls in and out of Manhattan for eight hours. In this incident, the New York Mercantile Exchange and the Commodity Exchange had to shut down operations.[20]
- Electronic intruders have shown the abilities to service control points, service provisioning systems, cross-connect systems, modify user services, forward calls, modify service class on circuit, turn off billing on specific circuits and routing tables, and service descriptions. Scott Maverick compromised 911 services in 1992. He was

arrested for tampering with these systems in Virginia, Maryland, and New Jersey. Maverick said his intent was to infect the 911 computer with a virus to cause havoc. "Significant degradation of service for 911 systems is possible if they are targeted by electronic intruders."[21]

- An April 1991 effort for a complete computer and telephone system invasion was the most comprehensive, coordinated attack on the PSN to date. Kevin Poulson pleaded guilty to all but one of the following counts: compromised an ongoing law enforcement investigation; identified law enforcement-run businesses and law enforcement wiretaps; intruded on the local exchange carrier (LEC) service-provisioning system numerous times (allegedly more than 40); modified existing telephone services, added new telephone services (some without billing), forwarded calls to other numbers, and dual-provisioned telephone lines; intruded on LEC maintenance/test systems to electronically monitor telephone conversations; intruded on LEC databases and obtained telephone numbers (some unlisted), street addresses, customer names, and other sensitive data; physically broke into carrier offices and stole equipment, software, identification badges, and other material; sold sensitive data obtained from LEC databases and illegally established or modified telephone services for other individuals; manufactured false identification, including telephone company identification badges and drivers licenses; intruded on other computer systems for profit, including the California Department of Motor Vehicles, credit bureaus, and an Air Force computer network; illegally possessed classified documents (the one count on which he pleads not guilty); and laundered money. Although Poulsen did not attack PSN networks, he did manipulate the system to his own ends and to his own personal profit.[22]

Viruses

Computer viruses can disrupt tactical operations. Trends in military electronics systems make them more vulnerable. "There is a concerted effort in the former Soviet client states to perfect computer crimes. There are universities . . . that teach how to create more effective viruses."[23] There is limited direct evidence and substantial indirect evidence that disruption technology exists in many nations: the former USSR, the United States, Bulgaria, Poland, Germany, the Netherlands, Italy, Canada, the United Kingdom, Taiwan, Sweden, Israel, Spain, and Australia (among others). It is clear from computer virus information alone that many countries of security interest to the United States have knowledge and technology to corrupt computer and network data and disrupt operations. Among them are India, Taiwan, Republic of Korea, China, Japan, and South Africa.

- A November 1988 virus (Morris Worm), placed on the Internet by a college student, infected 6,000 host computers in less than two hours and cost between $100,000 and $10 million to clean up, affecting network links between the Massachusetts Institute of Technology, University of California, Sandia National Laboratories, Lawrence Livermore National Laboratories, Los Alamos National Laboratory, and others.[24]
- A Christmas card message sent over BitNet, a global academic network, landed in 2,800 machines in five minutes, including IBM's internal network. It took only five

hours for the benign virus to spread 500,000 infections worldwide, forcing IBM to take the network down for several hours to accomplish repairs.[25]

- In 1992, Novell released a virus to thousands of customers in shrink-wrapped software due to a procedural error. The master disk was infected by a virus due to mishandling and failure to adhere to company policy during transportation to the disk duplication center.[26]
- Multiple books have been written on software viruses, including tutorials on how to write viruses aimed at military-use software. An interactive CD-ROM movie *Soft Kill* released in 1993 illustrates information warfare against the United States. It details corrupting time standards, affecting precision-guided weapon targeting and also targeting long distance telephone switches.[27] Tom Clancy's book *Debt of Honor* has a central theme of crippling information warfare attacks on the United States by means of viruses, worms, logic bombs, high energy radio frequency (HERF) guns, and ElectroMagnetic Pulse Transformer (EMP/T) bombs. The author's examples are not considered as malicious or as subtle as a real attack by experts would be.

Hackers

Hackers are the first group to learn of US vulnerabilities and are quick to share the information. Hacker magazines routinely tell hackers how to build and plant viruses, break into computer networks through access to telecom circuits, and gain entry to government networks. The Defense Information Systems Agency (DISA) has detected unknown intruders gathering Internet passwords through "sniffer" programs. In one 1994 observation period they estimated the number of captured passwords "at a million or more, potentially threatening all the host computers on the Internet and their users."[28] In another test, DISA conducted a test of logistics and medical network vulnerabilities in which the agency attacked 9,000 computers and successfully hacked 88 percent of them. Only 4 percent of successful attacks were detected.[29] Network administrators at the Air Force Information Warfare Center said they could crack 70 percent of the passwords on their UNIX network with tools resembling those now being used by Internet hackers.[30]

- National Aeronautics and Space Administration's (NASA) information technology security program manager, Rick Carr, said there are about 1,000 network break-in attempts a month, nearly fourfold over the last two to three years. Since November of last year, NASA documented six "high impact" attacks that have compromised sensitive or classified information. Losses were put at more than $250,000 per incident. Intrusions have resulted in theft and damage of research data.[31]
- Computer hackers infiltrated General Electric's (GE) computers, gaining access to research and proprietary information. The intruders managed to penetrate robust security barriers known as firewalls. The hackers had also obtained passwords of workers who were using GE computers to connect to more than a dozen Internet computers. The GE spokesperson said "We just know we were compromised."[32]
- An MCI employee was charged with stealing 100,000 calling card numbers and used them to place $50 million worth of fraudulent calls. The employee wrote software to

capture card numbers from various carriers that used MCI's switching equipment. He sent the captured numbers to an international hacker ring.[33]

- On 13 January 1995, the Naval Academy network had to be shut down due to password-sniffing software in one-third of its servers. The network is used by faculty, staff, and midshipmen. The academy was unable to determine how many passwords were collected or if the intruders had used the network as a launch pad into other DOD or federal systems.[34]

There are several hacking groups in Europe that keep lists of US military C2, research, and logistics computer accounts attained through hundreds of military Internet connections. The list is easily accessible.

- Project RAHAB is the German government's computer espionage program. Beginning in 1988 as an ongoing computer intrusion research effort, its primary focus is on cataloging network addresses and establishing pathways for later use. Its technicians have allegedly accessed computers in Russia, Japan, France, the United States, Italy, and Britain.[35]
- The Hannover hackers are a European hacking group that have been linked to the KGB. They gained illicit entry to over two dozen classified computer systems (as well as many others that were unclassified), and were caught when a 75-cent billing error was discovered at the Livermore Laboratories in Berkeley, California. The leader, Markus Hess, was able to acquire "superuser" status on network and surreptitiously stole authorized passwords for later exploitation. He penetrated the "Dockmaster" computer security database at the National Computer Security Center, a component of the National Security Agency. The case is rare where state-sponsored espionage has been acknowledged. Numerous other intrusions have been noticed and the frequency of intrusions is increasing.[36]
- Shortly after Iraq's invasion of Kuwait in 1990, a large-scale effort was launched worldwide to penetrate various sensitive US government and military computers. Although most of the penetrations originated in the Netherlands, an Iraqi intelligence operation against the North Atlantic Treaty Organization (NATO) was uncovered at the same time. The Dutch hackers penetrated host computers at Lawrence Livermore Laboratories in the United States and then branched out, penetrating computer systems at 34 DOD sites by weaving their way through university, government, and commercial systems on the Internet. They exploited a security hole in the Trivial File Transfer Protocol, which allowed users on the Internet to access a file containing encrypted passwords without logging onto the system.[37] The hackers were in a position to sell the gathered intelligence, either directly or indirectly, to Iraqi intelligence.[38] Dutch hackers successfully penetrated US military computer systems at least 34 times between April 1990 and May 1991. Pentagon officials report these same hackers offered to disrupt the US military's deployment to the Middle East in return for payment from Saddam Hussein in the amount of $1 million. Saddam spurned the offer.[39]
- Another case of hacking for possible espionage purposes involved a 16-year-old British cracker with the Internet name "Datastream" who cracked into South Korea's nuclear secrets via the Air Development Center at Griffiss Air Force Base, New York. He obtained information on North Korea's missile firing sites, aircraft design,

and psychological—on the world's business community.[47] There have been a number of bombs set off in London between 1990 and 1996 to make similar political statements.

- The World Trade Center bombing of February 1993 is another example of physical destruction to make a political statement. The goal was to shut down the New York financial system. There were six killed and over 1,000 injured; however, there were no serious systems losses, due to back-up system operation.
- Investigation of the 1995 train wreck in an isolated portion of the Arizona desert revealed a computer-monitored safety device had been short-circuited. The system was designed to warn of sequential loose rails but failed to operate because of apparent intentional tampering.

Notes

1. Science Applications International Corporation (SAIC), *Planning Considerations for Defensive Information Warfare-Information Assurance* (Washington, D.C.: SAIC, 16 December 1993), 16.
2. SAIC, *Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance* (Washington, D.C.: SAIC, 1995), 2-7.
3. William S. Sessions, "Computer Crimes An Escalating Crime Trend," *FBI Law Enforcement Bulletin,* February 1991, 12.
4. "Net Profit Or Loss," *Security Awareness News,* October 1995, 8–10.
5. Saul Hansell, "Citibank Fraud Raises Computer Security Questions," *New York Times,* 19 August 1995; John Alger, "Information Warfare: Hackers, Crackers, and the Projection of Power," address to the Third Tuesday Seminar Series, George Washington University, Washington, D.C., 17 October 1995.
6. Senate, Committee on Foreign Relations, *Hearings on the Subcommittee on Terrorism, Narcotics, and International Operations,* Washington, D.C.: Government Printing Office (GPO), 20–21 April 1994, 103–606. Testimony of R. James Woolsey, Director of Central Intelligence.
7. James Smith, "Logic Flaw is the Culprit in Computer Mugging," *Government Computer News,* 7 November 1994.
8. Winn Schwartau, *Information Warfare: Chaos on the Electronic Super Highway* (New York: Thunder's Mouth Press, 1994), 116.
9. SAIC, B-58.
10. Congress and Senate, Office of Technology Assessment, *Information Security and Privacy in Network Environments* (Washington, D.C.: GPO, September 1994), 3.
11. "Former IRS Worker Admits Snooping," *Boston Globe,* 5 April 1996.
12. Congress and Senate, Office of Technology Assessment, 2.
13. United States, National Communications System, *The Electronic Intrusion Threat to National Security and Emergency Preparedness Telecommunications: An Awareness Document* (Arlington, Va.: National Communications System, 1994), 2-13, 2-14.
14. Ibid., 2-13.
15. Neil Munro, "The Pentagon's New Nightmare: An Electronic Pearl Harbor," *Washington Post,* 16 July 1995, sec. C; SAIC, *Information Warfare,* 2-70.
16. SAIC, *Planning Considerations for Defensive Information Warfare,* 36–37.
17. Ibid.
18. United States, General Accounting Office (GAO), *Information Superhighway: An Overview of Technology Challenges* (Washington, D.C.: GAO, 23 January 1995), 36.
19. SAIC, *Planning Considerations for Defensive Information Warfare,* 37.
20. United States, GAO, *Information Superhighway: An Overview of Technology Changes,* 37.
21. United States, National Communications System, *The Electronic Intrusion Threat,* 4-3, 4-5.
22. Ibid., 2-9, 2-10.
23. Pat Cooper, "Organized Crime Hackers Jeopardize Security of U.S.," *Defense News,* 3 October 1994.

and US agents in North Korea. Richard Price, a London music student was charged with 12 offenses of unlawfully gaining access to USAF Lockheed/Martin computers. Following a 13-month US/UK intelligence agency operation, Price was arrested by UK police. He gained access on at least 69 occasions.[40]

- In 1995–96, an Argentine graduate student in Buenos Aires broke into sensitive US military and NASA files after gaining access through Harvard University, the University of Massachusetts, and Northeastern University computers. Julio Ardita breached computer security by obtaining passwords through a sniffer program that he transmitted to Harvard and other sites through the Argentine telephone system, Telecom. After obtaining the password to Telecom, he was able to break into computer systems run by US universities, the US Navy, other US agencies, and other computers in Korea, Mexico, Taiwan, Chile, and Brazil.[41]
- The USSR succeeded in gaining access to production information on the NATO "Tornado" jet fighter in 1984 by accessing databases of the Messerschmitt-Bolkow-Blohm company in Munich. Soviet computer hacking involved some 2.4 percent of overall Soviet espionage operations in 1983.[42]
- DST, the French government's electronic data collection program, has a "hot list" of firms targeted for electronic monitoring including IBM, Dow Chemical, General Electric, Corning, Texas Instruments, AT&T, GTE, Du Pont, Siemens, Hitachi, Fujitsu, Sony, Bosch, BASF, and Boeing.[43]
- German intelligence agents managed to illegally access hundreds of computers worldwide through NASA's SPAN network. They managed to break into the CERN (European Laboratory for Particle Physics) physics laboratory computer system in Geneva and loaded a damaging Trojan Horse that destroyed software and crashed systems.[44]
- There is growing evidence of the use of electronic intrusion techniques by industrial spies. In a survey of 150 high-technology research and development companies, 48 percent said they had been the target of trade secret theft. Kevin Mitnick was arrested and prosecuted in 1989 for stealing more than $1 million in source code from Digital Equipment Corporation (DEC), modifying it to add "trap doors," and attempting to copy it back to DEC's development computers.[45]

Destruction (Physical Attacks)

The globalized digital information system offers lucrative targets in a terrorist's strategy of destabilizing the sociopolitical order. The terrorist chooses people as his most effective target, to influence, rather than kill them, by attacking targets that affect the largest number of people, thus attracting publicity. In Japan, terrorists have attacked the computerized control systems for commuter trains, paralyzing major cities for hours. In Italy, the Red Brigade's manifesto specified the destruction of computer systems and installations "for striking at the heart of the state."[46]

- On 10 April 1992, the Irish Republican Army (IRA) set off a bomb in the Square Mile of London. Though three people were killed, the intent was not to kill; it was an attack on the financial center of Europe, causing severe effect—electronic, financial,

24. Philip Elmer-DeWitt, "The Kid Put Us Out of Action," *Time,* 14 November 1988, 76. SAIC, *Information Warfare Assurance,* 2-7.

25. Lawrence J. Haas, "NII Security: The Federal Role," draft (Washington, D.C.: National Information Infrastructure Security Issues Forum, 14 June 1995), 18.

26. SAIC, *Planning Considerations for Defensive Information Warfare*, 37.

27. "Soft Kill" (Interactive CD-ROM) XIPHAS, 1993.

28. Congress and Senate, Office of Technology Assessment, 3.

29. Neil Munro, "New Information War Doctrine Poses Risks, Gains," *Washington Technology* 9, no.18 (22 December 1994):1.

30. Sharon P. McCarthy, "Network Break-ins Reveal the Chinks in Systems Security," *Government Computer News,* 8 August 1994.

31. Elizabeth Sikorovsky, "Internet Break-ins Compromise Hacker Attack," *Federal Computer Week,* 19 December 1994, 4.

32. Jared Sandberg, "GE Says Computers Linked to Internet Were Infiltrated," *The Wall Street Journal,* 28 November 1994, sec. B.

33. Joseph C. Panettieri, "Are Your Computers Safe?" *Information Week,* 28 November 1994, 3.

34. Bob Berwin, "Naval Academy Network Stung by Hacker Attack," *Federal Computer Week* 9, no. 2, 23 January 1995, 3.

35. Peter Schweizer, *Friendly Spies: How America's Allies Are Using Economic Espionage to Steal Our Secrets* (New York: Atlantic Monthly Press, 1993), 158; and Wayne Madsen, "Intelligence Agency Threats to Computer Security," *International Journal of Intelligence and Counterintelligence* 6, no. 4 (Winter 1993): 421.

36. Madsen, 418; Alger, 6; and SAIC, *Information Warfare*, 2-68.

37. Congress and Senate, Office of Technology Assessment, 2.

38. Madsen, 437–88.

39. Douglas Waller, "Onward Cyber Soldiers," *Time,* 21 August 1995, 43.

40. Neal Pollard, "Computer Terrorism," address to the 1995 International Information Warfare Conference, Arlington, Va., 7 September 1995.

41. Bob Hohler and Hiawatha Bray, "Computer Wiretap Helps Track Hacker," *Boston Globe,* 30 March 1996; and "Hacker Boasted of Access to US Computers, Newspaper Says," *Boston Sunday Globe,* 31 March 1996.

42. Madsen, 419.

43. Ibid., 422.

44. Ibid., 421.

45. United States, National Communications System, *The Electronic Intrusion Threat*, 2-5, 2-18.

46. Pollard, 6.

47. Ibid., 13.

Appendix B

The Day After . . . In Cyberspace

No.	Incident Description
1.	May 7 - Iran announces it would soon begin conducting military exercises "appropriate to the evolving security situation in the Gulf."
2.	May 10 - Tehran radio and TV announced that Iranian Foreign Minister was flying to Riyadh, Saudi Arabia, with an "urgent proposal" that would "resolve the OPEC stalemate" and "respond to the evolving security situation in the region."
3.	May 11 - 90 percent of the power in the Cairo, Egypt, area went out for several hours. Cause—unknown.
4.	May 11 - The public switched network (PSN) for northern California and Oregon suffers a series of massive failures. Cause—trap door.[1]
5.	May 11 - The base phone system in Fort Lewis, Washington, is subjected to a mass dialing attack by personal computers.
6.	May 13 - The largest ARAMCO refinery near Dhahran, Saudi Arabia, has a catastrophic flow control malfunction, which leads to a large explosion and fire.
7.	May 14 - Iran sends messages to Gulf Coordinating Council (GCC) members, the United States, the United Kingdom, and France calling for negotiations. Messages sent to the Kuwait and Saudi leaders state Iran will soon "demonstrate the futility of depending upon the American imperialists for protection from modern weapons systems."
8.	May 14 - A new, high-speed Metro-Superliner traveling at 300 km/hr slams into an apparently misrouted freight train near Laurel, Maryland. The wreck kills over 60 passengers and crew and injures another 120. Cause—logic bomb.[2]
9.	May 15 - The Iranian ambassador to the United Nations (UN) is overheard to state that as United States is "the technologically most advanced power on the planet," it is highly vulnerable to "21st century attacks" by "states and others who had mastered contemporary computer and telecommunication technology."
10.	May 16 - Scotland Yard informs the Prime Minister that the Bank of England had detected "three different sniffer devices[3] of a new design in its main funds transfer system" and bank officials were fearful that unauthorized individuals could now enter the funds transfer system.
11.	May 16 - Cable News Network (CNN) airs a "Special Report" that features the Metroliner train wreck and leaked reports about the Bank of England. CNN states "some Western intelligence agencies" believe that Iran may be employing

computer experts from the Russian Mafia and "renegade software writers" from India to "threaten the entire economic fabric of the United States and West Europe." Thereafter, the London Stock Exchange Index falls 10 percent and the New York Stock Exchange suffers its largest drop since the crash of 1987. Business news networks speculate the losses are caused by major institutional investors attempting to get out of the electronically managed market. The Security and Exchange Commission reports a pattern of institutional investment manipulation involving unknown parties working through European and Middle Eastern Banks.

12. May 17 - The Consortium for Planetary Peace (CPP) announces that an "emergency mobilization to stop an unnecessary and potentially devastating war" will take place in 48 hours. Two hours later, it files a request with the US Park Police for a permit for the Mall to accommodate an estimated 100,000 participants.

13. May 20 - The Senate, in the face of an aggressive lobby campaign by CPP passes by two votes, a resolution supporting the president's decision to send troops to the Gulf.

14. May 20 - DOD discovers there is corrupt data in the time-phased force deployment list (TPFDL).

15. May 20 - The automatic tellers of the two largest bank chains in Georgia start to malfunction with bank clients being debited and/or credited thousands of dollars after each automated teller machine (ATM) transaction. By midday, they shut down their ATM machines.

16. May 20 - CNN airs a "Special Report" focused on the vulnerability of the United States to "cyberspace warfare"—dwelling on the Metroliner crash, the telephone outage in the Northwest, the ATM malfunctions, and the interference with CNN's own transmissions. Interviews accompanying the program convey a growing sense of public concern that the United States was far more vulnerable to information warfare (IW) attack than "the government has told us."

17. May 21 - The Russian Foreign Minister criticizes the United States and allied deployments to the Gulf as "dangerous brinkmanship" and offers to host an international summit to defuse the crisis.

18. May 21 - The CPP "anti-intervention" demonstration in Washington far exceeds expectations and draws 400,000 people.

19. May 22 - The pilot of a new Continental Airlines AB-340 jet making a final approach to O'Hare International Airport reports his flight deck avionics has suffered a massive malfunction and the aircraft is out of control. It crashes, killing 30 and injuring another 100 people. A report concludes the AB-340 and 330 flight-control software may be infected by a sophisticated logic bomb and the Federal Aviation Administration (FAA) grounds all such aircraft.

20. May 23 - The news anchors of the Saudi government's networks were suddenly replaced by the face of the head of the CIRD Council who called on the citizens of Saudi Arabia "to join forces in the peaceful transformation of the Saudi kingdom to freedom and democracy under Islam." The prearranged signal leads to large-scale demonstrations against the Saudi monarchy.

21. May 23 - The Saudi PSN network begins to fail apparently due to unauthorized modification of the system through a trap door.

22. May 23 - The local television station in Dhahran, Saudi Arabia, announces that the "Provisional Islamic Republic of Arabia" had seized power in Dhahran and Mecca. He states that Iranian military assistance "would be immediately halted if foreign nations let the Arabian revolution proceed on its own."

23. May 23 - The Secretary of Defense is informed that a full-scale IW attack of unknown sources is underway at "almost every military base in the United States and Europe" involved in the deployment to Saudi Arabia.

24. May 24 - At a news conference held at the CNN newsroom, the CPP denounces the "criminal action which led to the Airbus tragedy at O'Hare" but concluded that "legitimate protest should not be quashed by the terrorist acts of a few." It announces it was "mobilizing all of its chapters to conduct civil disobedience actions to stop the US government's mad dash to war to save an undemocratic and failed Saudi regime."

25. May 24 - Several joint surveillance, target attack radar system (JSTARS) aircraft operating in the Gulf region appear to be plagued with a computer worm[4] triggered by some external source.

26. May 24 - The entire phone network in the Washington/Baltimore region including local cellular systems fails. A preliminary assessment suggests an attack through a trap door has caused it.

27. May 24 - The Chicago Commodity Exchange experiences some of its "wildest fluctuations in history." There is widespread suspicion that "the Exchange was being subjected to a powerful form of electronic manipulation by parties unknown."

28. May 24 - CBS Evening News was interrupted for seven minutes by the "Action Arm of the Committee for Planetary Peace." During the video takeover, the CPP spokesperson, a well-known and highly regarded media personality, called for widespread civil disobedience to thwart an administration that has "lost touch with domestic and international reality."

Figure B.1 lists incidents, types of attacks, weapons categories, and target centers of gravity from the RAND war game.

Incident Number	Type of Attack	Weapons Category	Target Center of Gravity
1. Iranian Exercises	Persuasion	Perception Management	Leaders
2. Iranian Diplomatic Initiative	Persuasion	Perception Management	Leaders
3. Cairo Power Outage	Logic Bomb	Corruption	System Essentials
4. California/Oregon PSN Shutdown	Trap Door	Corruption	System Essentials
5. Ft. Lewis Mass Dialing Attack	Info Overload	Corruption	Defense Mechanism
6. ARAMCO Explosion	Logic Bomb	Corruption	System Essentials
7. Iran Message to Gulf Coordinating Council	Persuasion	Perception Management	Leaders
8. Metroliner Crash	Logic Bomb	Corruption	Infrastructure
9. Iranian Ambassador Statement	Discourse	Perception Management	Leaders
10. Bank of England	Sniffers	Corruption	System Essentials
11. CNN "Financial Targets" Report	Persuasion	Perception Management	Population
12. CPP Press Release	Slogans	Perception Management	Population
13. Close Vote in Senate	Argument	Perception Management	Leaders
14. TPFDL Pollution	Virus	Corruption	Defense Mechanism
15. Bank ATMs Malfunction	Logic Bomb	Corruption	System Essentials
16. CNN Government Coverup Report	Persuasion	Perception Management	Population
17. Russian Diplomatic Initiative	Persuasion	Perception Management	Leaders
18. CPP Demonstration	Slogans	Perception Management	Leaders
19. Airplane Crash	Logic Bomb	Corruption	Infrastructure
20. Saudi News Takeover	Spamming	Perception Management	Population
21. Saudi PSN Shutdown	Logic Bomb	Corruption	System Essentials
22. Saudi TV Announces Coup	Misinformation	Perception Management	Population
23. IW Attacks Against US Bases	Multiple Efforts	Corruption	Defense Mechanism
24. CPP News Conference	Argument	Perception Management	Population
25. JSTARS Malfunction	Worm	Corruption	Defense Mechanism
26. D.C./Baltimore Phone Shutdown	Logic Bomb	Corruption	System Essentials
27. Chicago Exchange Fluctuations	Logic Bomb	Corruption	System Essentials
28. CBS News Takeover	Spoofing	Perception Management	Population

Legend:
ATM - automated teller machine
CNN - Cable News Network
CPP - Consortium for Planetary Peace
IW - Information Warfare
JSTARS - joint surveillance, target attack radar system
PSN - Public Switch Network
TPFDL - time-phase force deployment list

TOTALS:

WEAPON TYPES

Destruction - 0
Corruption - 14
Perception Management - 14

CENTERS OF GRAVITY TARGETED

Leaders - 7
System Essentials - 8
Infrastructure - 2
Population - 7
Defense Mechanism - 4

Figure B.1. Illustrative Incidents from RAND War Game "The Day After . . . in Cyberspace"

The capabilities required to produce the incidents used in the RAND "Day After" exercise have, for the most part, already been seen. Figure B.2 attempts to provide examples of similar real-world events for each technology-related incident in the war game.

The assumption of the exercise is that a malevolent actor intentionally assembles these capabilities in a structured attack. The Kevin Poulsen details, provided in item 21, show some blending of capacity and intent. Individual account descriptions are provided below.

Incident Number	Type of Attack	Similar World Event
3. Cairo Power Outage	Logic Bomb	Computer Espionage
4. California/Oregon Public Switch Network (PSN) Shutdown	Trap Door	Legion of Doom Time Bomb
5. Ft. Lewis Mass Dialing Attack	Info Overload	Noted Intruder Skills
6. ARAMCO Explosion	Logic Bomb	Kevin Poulsen Pleads Guilty
8. Metroliner Crash	Logic Bomb	1995 Arizona Railway Incident
10. Bank of England	Sniffers	Citibank $10 Million Fraud Case
14. Time-Phase Force Deployment List Pollution	Virus	Paid Informants
15. Bank Automated Teller Machines Malfunction	Logic Bomb	$70 Million Software Glitch
19. Airplane Crash	Logic Bomb	Disgruntled Defense Contractor Employee
20. Saudi News Takeover	Spamming	Demonstrated Technology
21. Saudi PSN Shutdown	Logic Bomb	Kevin Poulsen Pleads Guilty
23. Information Warfare Attacks Against US Bases	Multiple Efforts	Defense Information Systems Agency Red Team Results
25. Joint Surveillance, Target Attack Radar System Malfunction	Worm	Electronic Intruders
26. D.C./Baltimore Phone Shutdown	Logic Bomb	Other Phone System Failures
27. Chicago Exchange Fluctuations	Logic Bomb	Shutdown Options
28. CBS News Takeover	Spoofing	Demonstrated Technology

Figure B.2. RAND War Game Incident Comparison

Figures B.3 and B.4 place these illustrative incidents in a framework and identify where the effects of information weapons fall.

	Leaders	System Essentials	Infrastructure	Population	Defense Mechanism
Destruction Physical destruction					
Corruption Internal operating logic		3 Cairo Power 4 California/Oregon Public Switch Networks (PSN) 6 ARAMCO 10 Bank of England 15 Automated Teller Machines 21 Saudi PSNs 26 D.C./Baltimore PSN 27 Chicago Trade	8 Metroliner 19 Airplane		5 Ft. Lewis 14 TPFDL 23 Information Warfare Attacks 25 Joint Surveillance, Target Attack Radar System
Perception Management Behavior	1 Iran Exercise 2 Iranian Diplomatic Initiative 7 Iran Message 9 Iran Ambassador 13 Senate Vote 17 Russia Diplomatic Initiative 18 Consortium for Planetary Peace (CPP) Demo			11 Cable News Network (CNN) Report 12 CPP Press Release 16 CNN Report 20 Saudi News 22 Saudi Coup 24 CPP News 28 CBS News	
Ignore					

Figure B.3. Illustrative Information Incidents Placed in Framework

	Leaders	System Essentials	Infrastructure	Population	Defense Mechanism
Destruction Physical destruction		6 ARAMCO	8 Metroliner 19 Airplane	8 Metroliner 19 Airplane	
Corruption Internal operating logic		3 Cairo Power 4 California/Oregon PSNs 5 Ft. Lewis 6 ARAMCO 10 Bank of England 15 ATMs 21 Saudi PSNs 23 IW Attacks 26 D.C./Baltimore PSN 27 Chicago Trade	8 Metroliner 19 Airplane	3 Cairo Power 4 California/Oregon PSNs 15 ATMs 21 Saudi PSNs 26 D.C./Baltimore PSN 27 Chicago Trade	5 Ft. Lewis 14 TPFDL 23 IW Attacks 25 JSTARS
Perception Management Behavior	1 Iran Exercise 2 Iranian Diplomatic Initiative 3 Cairo Power 4 California/Oregon PSNs 5 Ft. Lewis 6 ARAMCO 7 Iran Message 8 Metroliner 9 Iran Ambassador 10 Bank of England 11 CNN Report 12 CPP Press Release 13 Senate Vote 14 TPFDL 15 ATMs 16 CNN Report 17 Russia Diplomatic Initiative 18 CPP Demonstration 19 Airplane 20 Saudi News 21 Saudi PSNs 22 Saudi Coup 23 IW Attacks 24 CPP News 26 D.C./Baltimore PSN 27 Chicago Trade 28 CBS News			8 Metroliner 10 Bank of England 11 CNN Report 12 CPP Press Release 15 ATMs 16 CNN Report 19 Airplane 20 Saudi News 21 Saudi PSNs 22 Saudi Coup 24 CPP News 26 D.C./Baltimore PSN 27 Chicago Trade 28 CBS News	5 Ft. Lewis 14 TPFDL 23 IW Attacks 25 JSTARS
Ignore					

Legend:
ATM - automated teller machine
CNN - Cable News Network
CPP - Consortium for Planetary Peace
IW - Information Warfare
JSTARS - joint surveillance, target attack radar system
PSN - Public Switch Network
TPFDL - time-phase force deployment list

Figure B.4. Using the Framework to Identify Where the Effects of Information Weapons Fall

Corresponding Real World Incident Descriptions*

3. Computer Espionage - German intelligence agents managed to illegally access hundreds of computers worldwide through NASA's SPAN network. They broke into the European Laboratory for Particle Physics (CERN) physics laboratory computer system in Geneva and loaded a damaging Trojan Horse that destroyed software and crashed systems.[5]

4. Legion of Doom's (LOD) PSN Time Bombs - In 1990, several Atlanta branch LOD members were arrested on charges of penetrating and disrupting telecommunication network elements. Federal agents accused the LOD members of planting a series of destructive "time bomb" programs in network elements in Denver, Colorado; Atlanta, Georgia; and New Jersey. These time bombs were designed to shut down major switching hubs, but were defused by telephone company employees before they caused damage. "Based on an analysis of open source literature, the author believes that groups of electronic intruders, if organized and funded by interested adversaries, have the capabilities to launch sophisticated widespread attacks on and across the PSN. These types of attacks could result in significant degradations in the nation's NS/EP telecommunication capabilities, create significant public health and safety problems, and cause serious economic shocks."[6]

5. Noted Intruder Skills - Electronic intruders have shown the abilities to service control points, service provisioning systems, cross-connect systems, modify user services, forward calls, modify service class on circuit, turn off billing on specific circuits, routing tables, and service descriptions. Scott Maverick compromised 911 services in 1992. He was arrested for tampering with these systems in Virginia, Maryland, and New Jersey. Maverick said his intent was to infect the 911 computer with a virus to cause havoc. "Significant degradation of service for 911 systems is possible if they are targeted by electronic intruders."[7]

6. Kevin Poulsen Pleads Guilty - Allegedly masterminded an April 1991 effort for a complete computer and telephone system invasion. The most comprehensive, coordinated attack on the PSN to date. Pleaded guilty to all but one of the following counts: compromised an ongoing law enforcement investigation; identified law enforcement-run businesses and law enforcement wiretaps; intruded on local exchange carrier (LEC) service provisioning system numerous times (allegedly more than 40); modified existing telephone services, added new telephone services (some without billing), forwarded calls to other numbers and dual-provisioned telephone lines; intruded on LEC maintenance/test systems to electronically monitor telephone conversations; intruded on LEC databases and obtained telephone numbers (some unlisted), street addresses, customer names, and other sensitive data; physically broke into carrier offices and stole equipment, software, identification badges, and other material; sold sensitive data obtained

* Numbered real-world incident descriptions in this section correspond to war game incident description numbers in the preceding section.

from LEC databases and illegally established or modified telephone services for other individuals; manufactured false identification, including telephone company identification badges and drivers licenses; intruded on other computer systems for profit, including the California Department of Motor Vehicles, credit bureaus, and an Air Force computer network; illegally possessed classified documents (the one count on which he pleads not guilty); and laundered money. Although Poulsen did not attack PSN networks, he manipulated the system to his own ends and to his own personal profit.[8]

8. Arizona Railway Incident - Investigation of the 1995 train wreck in an isolated portion of Arizona desert revealed a computer-monitored safety device had been short-circuited. The system was supposed to warn of sequential loose rails but failed to operate because of apparently intentional tampering.

10. Citibank $10 Million Fraud Case - A 34-year-old Russian, operating from Saint Petersburg, managed to gain access codes and move $10 million in funds from Citibank accounts in Argentina and Indonesia. Combine this capability with a 1994 case at a California university where an unauthorized program collected tens of thousands of account names and passwords through a "sniffer" program on the Internet before it was found.[9]

14. Paid Informants - National Communications System (NCS) says there is significant evidence of insiders selling information to information brokers, industrial spies, criminal organizations, and intelligence services. These insiders, with full access to their respective information files, have provided data on unpublished telephone numbers, toll records, credit reports, and other personal data. The FBI reported that criminal organizations have gained access to the National Crime Information Center records primarily through the use of compromised employees. In December 1991, 18 Social Security Administration employees were indicted for sale of confidential information.[10]

15. $70 Million Software Glitch - A $70 million government loss due to overpayment by the Health Care Financing Administration was caused by a software problem that failed to cross-check Medicaid-eligible people against Medicaid claims. The money was spent for services provided; however, not all patients were eligible. The largest organization overpayment was $19 million.[11]

19. Disgruntled Defense Contractor Employee - In August 1992, a computer systems administrator for a defense contractor was told of a pending layoff. The employee set up a malicious code to activate after his departure. He hoped that the company would hire him back to reconstruct databases after the logic bomb functioned. His attempt was discovered before he left and he later pleaded guilty to the charge. If the malicious code had functioned, substantial data on the development of military missile systems would have been destroyed and would have required months to reprogram the computer system.[12]

21. See item six.

23. Defense Information Systems Agency (DISA) Red Team Results - The team attempted to gain access to 9,000 computers across the defense department. They successfully hacked into 88 percent, over 7,900, of the computers. They left signs of their trespass yet only just over 300 of the illegal entries were detected. Network administrators at the Air Force Information Warfare Center said they could crack 70 percent of the passwords on their UNIX network with tools resembling those now being used by Internet hackers.[13]

25. Electronic Intruders - There is growing evidence of the use of electronic intrusion techniques by industrial spies. In a survey of 150 high technology research and development companies, 48 percent said they had been the target of trade-secret theft. Combine this information with the case of Kevin Mitnick. He was arrested and prosecuted in 1989 for stealing more than $1 million in source code from Digital Equipment Corporation (DEC), modifying it to add "trap doors," and attempting to copy it back to DEC's development computers.[14] JSTARS is a highly software-dependent program that could be vulnerable to this type of intrusion.

26. Other Phone System Failures - A 1991 near-total shutdown of telephone service in the Baltimore-Washington area was caused by a coding error in new AT&T long-distance software. A highway crew digging post holes disrupted coast-to-coast calls by cutting a MCI fiber-optic cable. A similar incident in New Jersey cut 60 percent of the calls in and out of Manhattan for eight hours. In this incident the New York Mercantile Exchange and the Commodity Exchange had to shut down operations. Additionally, voice and radar systems used to control air traffic from facilities in New York, Washington, and Boston were disabled for five hours.[15]

27. See item 26 and other cases of software manipulation.

Notes

1. "A hidden software mechanism triggered to circumvent system security measures. This can be a legitimate programming technique that allows a developer to bypass lengthy log-on routines or access source code directly. Its existence, if known by unauthorized persons, however, can be the source of a significant security breach." *Definitions for the Discipline of Information Warfare and Strategy* (Washington, D.C.: School of Information Warfare and Strategy, National Defense University, July 1995), 79.

2. "A type of Trojan horse that may or may not be a virus. Its mission component is triggered by a true/false condition. Logic bombs do not propagate; they just sit and wait." A Trojan horse is a "malicious computer code that is located within a desirable block of code, (i.e., an application program, operating system software, etc.). To be a Trojan horse, the presence of the code must be unknown and it must perform an act that is not expected by the owner of the system," Ibid., 46 and 80.

3. Software programs designed to analyze a communications network. They diagnose problems and assist network administrators in fixing them. In some cases, the software is written so that network administrators are unaware someone else is snooping through the networks collecting information such as passwords, tapping databases, and listening in on telecommunications transmissions. Sniffers may be written to ferret out information which will permit the user to surreptitiously enter and/or manipulate the system later on. Winn Schwartau, *Information Warfare: Chaos on the Electronic Super Highway* (New York: Thunder's Mouth Press, 1994), 116.

4. A computer program that eats up the memory and resources of a computer, effectively rendering it useless. Schwartau, 120.

5. Wayne Madsen, "Intelligence Agency Threats to Computer Security," *International Journal of Intelligence and Counterintelligence* 6, no. 4 (Winter 1993): 421.

6. United States, National Communications System, *The Electronic Intrusion Threat to National Security and Emergency Preparedness: An Awareness Document* (Arlington, Va.: National Communications System, 1994), 2-5, 4-2.

7. Ibid., 4-3, 4-5.

8. Ibid., 2-9, 2-10.

9. Ibid., 3-4; and Saul Hansell, "Citibank Fraud Raises Computer Security Questions," *New York Times*, 19 August 1995.

10. United States, National Communications System, *The Electronic Intrusion Threat,* 2-13, 2-14.

11. Science Applications International Corporation (SAIC), *Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance* (Washington, D.C.: SAIC, 1995), B-96.

12. United States, National Communications System, *The Electronic Intrusion Threat*, 2-13.

13. SAIC, *Information Warfare,* B-66, B-72.

14. United States, National Communications System, *The Electronics Intrusion Threat*, 2-5, 2-18.

15. SAIC, *Information Warfare,* 36; United States Government Accounting Office (GAO), "Information Superhighway: An Overview of Technology Challenges," report to Congress (Washington, D.C.: GAO, 23 January 1995), 36.

Bibliography

Adams, James. "The Role of the Media." Lecture. Information Warfare Course, National Defense University, Washington, D.C., 17 December 1995.

Air Force. *The Nation's Air Force Booklet.* Washington, D.C.: Headquarters USAF, 1995.

Alberts, David S. Defensive Information War: Problem Formulation and Solution Approach. Washington, D.C.: National Defense University, 17 January 1996.

Alger, John. "Information Warfare: Hackers, Crackers and the Projection of Power." Address. 1995–1996 Third Tuesday Seminar Series: Interdisciplinary Aspects of the Electronic Superhighway. George Washington University, Washington, D.C., 17 October 1995.

Allard, Kenneth C. "The Future of Command and Control: Toward a Paradigm of Information Warfare." *Turning Point: The Gulf War and US Military Strategy.* Edited by L. Benjamin Ederington and Michael J. Mazaar. Boulder, Colo.: Westview Press, 1994.

Army Field Manual (FM) 100-5. *Operations.* Fort Monroe, Va.: TRADOC, 1993.

Army FM 100-6. "Information Operations." Draft. Fort Monroe, Va.: TRADOC, January 1996.

Army Field Manual. *Concept for Information Operations.* Fort Monroe, Va.: TRADOC, August 1995.

Arquila, John, and David Ronfeldt. "Cyberwar is Coming!" *Comparative Strategy* 12 (April–June 1993).

Arquila, John. "Information, Power and Grand Strategy: In Athena's Camp." Paper presented at the Catigny Conference. Wheaton, Ill., July 1995.

———. "Strategic Implications of Information Dominance." *Strategic Review,* Summer 1994.

Barnett, Jeff. *The Revolution in Military Affairs.* Briefing slides. Washington, D.C.: Department of Defense, Office of Net Assessment, 1995.

Boyd, John R. "A Discourse in Winning and Losing." Briefing at Maxwell AFB, Ala. Air University Library, 1987.

Brewin, Bob. "Naval Academy Network Stung by Hacker Attack." *Federal Computer Week* 9, no. 2 (23 January 1995).

Broder, David S. "Looking Ahead in '92." *Boston Globe,* 6 April 1994.

Brown, Michael. "Information Warfare." Lecture. Information Warfare Course. National Defense University, Washington, D.C., 17 December 1995.

———. "Information Warfare and the RMA." *Seminar on Intelligence and Command and Control.* Cambridge, Mass.: Center for Information Policy Research, Harvard University, January 1996.

Builder, Carl H. "Rethinking National Security and the Role of the Military." Unpublished article. Santa Monica, Calif.: RAND, 6 September 1995.

Center for Disease Control. *Addressing Emerging Infectious Disease Threats: A Prevention Strategy for the United States.* Atlanta, Ga.: Center for Disease Control and Prevention, April 1994.

Christopher, Warren, et al. *American Hostages in Iran: The Conduct of a Crisis.* New Haven, Conn.: Yale University Press, 1985.

Clausewitz, Carl von. *On War.* Edited and translated by Michael Howard and Peter Paret. Princeton, N.J.: Princeton University Press, 1976.

Cleveland, Harlan. *The Knowledge Executive: Leadership in an Information Society.* New York: Truman Talley Books, 1985.

Congress and House. Judiciary Committee. *Hearings on the Threat of Foreign Economic Espionage to US Corporations.* Washington, D.C.: Government Printing Office (GPO), 29 April–7 May 1992.

Congress and Senate. *Information Security and Privacy in Network Environments.* Washington, D.C. : GPO, September 1994.

———. *Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage.* Washington, D.C.: GPO, June 1990.

Conley, Robert. "Information Warfare-Some Thoughts." Unpublished paper, 1993.

Cooper, Jeffery. "Another View of Information Warfare: Conflict in the Information Age." Prepublication draft. Washington, D.C.: Science Applications International Corporation, 30 August 1995.

Cooper, Pat. "Organized Crime Hackers Jeopardize Security of U.S." *Defense News,* 3 October 1994.

Definitions for the Discipline of Information Warfare and Strategy. Washington, D.C.: School of Information Warfare and Strategy, National Defense University, July 1995.

deGraffenreid, Kenneth E., and Michelle Van Cleave. "Information Assurance and the Future of the NCS." Draft. Fairfax, Va.: National Security Research, Inc., 12 May 1995.

Department of Defense (DOD) Joint Publication 3-0. *Doctrine for Joint Operations.* Washington, D.C.: The Joint Staff, 1 February 1995.

Department of the Air Force. *Cornerstones of Information Warfare.* Washington, D.C.: Headquarters USAF, 1995.

Dunn, Richard J., III. *From Gettysburg to the Gulf and Beyond: Coping With Revolutionary Technological Change in Land Warfare.* Washington, D.C.: Institute for National Strategic Studies, 2 May 1992.

Edmunds, Albert. Interview. *Defense News,* 16 October 1995.

Elmer-DeWitt, Philip. "The Kid Put Us Out of Action." *Time,* 14 November 1988.

Executive Order 12148. Federal Emergency Management. 44 Federal Register 43239. Washington, D.C.: GPO, 20 July 1979.

Executive Order 12472. Assignment of National Security and Emergency Preparedness Telecommunications Functions. 49 Federal Register 13471. Washington, D.C.: GPO, 3 April 1984.

Executive Order 12656. Assignment of Emergency Preparedness Responsibilities. 53 Federal Register 226. Washington, D.C.: GPO, 18 November 1988.

Executive Order 12919. National Defense Industrial Resources Preparedness. 59 Federal Register 29525. Washington, D.C.: GPO, 3 June 1994.

Fairfield, John S. "A Jointly Focused Vision." *Armed Forces Journal,* January 1996.

Fogleman, Ronald R. "Information Operations: The Fifth Dimension of Warfare." Address. Armed Forces Communications Electronics Association, Washington, D.C., 25 April 1995.

Franks, Frederick M. Address. Association of United States Army Symposium, Orlando, Fla., 8 February 1994.

Garigue, R. "Information Warfare: Developing a Conceptual Framework." Draft. Ottawa: Office of the Assistant Deputy Minister, Defense Information Services, 23 August 1995.

Gertz, Bill. "French Spooks Scare Firms." *Washington Times,* 9 February 1992.

Grove, Ronald. "The Information Warfare Challenges of a National Infrastructure." Address. 1995 International Information Warfare Conference, INFOCON Symposium, Arlington, Va., 7 September 1995.

Haas, Lawrence J. "NII Security: The Federal Role." Address. National Information Infrastructure Security Issues Forum, Washington, D.C., 14 June 1995.

"Hacker Boasted of Access to US Computers, Newspaper Says." *Boston Sunday Globe,* 31 March 1996.

Hansell, Saul. "Citibank Fraud Raises Computer Security Questions." *New York Times,* 19 August 1995.

Hohler, Bob and Hiawatha Bray. "Computer Wiretap Helps Track Hacker." *Boston Globe,* 30 March 1996.

International Energy Agency. *The International Energy Agency Natural Gas Security Study.* Paris: Organization for Economic Cooperation and Development/International Energy Agency, 1995.

Jenner, Christopher. Faxed memorandum to authors, 5 March 1996.

Joint Security Commission. *Redefining Security*. Washington: Joint Security Commission, February 1994.

Libicki, Martin C. *The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon*. Washington, D.C.: Institute for National Strategic Studies, National Defense University, 1994.

———. *What is Information Warfare?* Washington, D.C.: Institute for National Strategic Studies, National Defense University, August 1995.

Lucky, Robert. *Silicon Dreams: Information, Man and Machine*. New York: St. Martin's Press, 1989.

Lykke, Arthur F. Lecture. Army War College, Carlisle Barracks, Pa., July 1995.

Madsen, Wayne. "Intelligence Agency Threats to Computer Security." *International Journal of Intelligence and Counterintelligence* 6, no. 4 (Winter 1993).

Mann, Edward. *Thunder and Lightning: Desert Storm and the Airpower Debates*. Maxwell Air Force Base, Ala.: Air University Press, 1995.

Marshall, Andrew W. Memorandum for the Record. Subject: "RMA Update." 2 May 1994.

McCarthy, Shawn P. "Network Break-ins Reveal the Chinks in Systems Security." *Government Computer News,* 8 August 1994.

McNulty, Thomas J. "Television's Impact on Executive Decision Making and Diplomacy." *Fletcher Forum on World Affairs* 17 (Winter 1993).

Molander, Roger C., Andrew S. Riddile, and Peter A. Wilson. "Strategic Information Warfare: A New Face of War." Draft. Santa Monica, Calif.: RAND, 1995.

Morton, Oliver. "The Information Advantage." *The Economist,* 10 June 1995.

Munro, Neil. "New Information Warfare Doctrine Poses Risks, Gains." *Washington Technology* 9, no. 18 (22 December 1994).

———. "The Pentagon's New Nightmare: An Electronic Pearl Harbor." *Washington Post*. 16 July 1995.

National Research Council. *Computers at Risk: Safe Computing in the Information Age*. Washington, D.C.: National Academy Press, 1991.

———. *Growing Vulnerability in Public Switched Networks: Implications for National Security Emergency Preparedness*. Washington, D.C.: National Academy Press, 1991.

National Security Telecommunications Advisory Committee (NSTAC). *Report to NSTAC XVIII*. Washington, D.C.: National Information Infrastructure Task Force, February 1996.

Neilson, Robert E. "The Role of Information Technology in National Security Policy." *Acquisition Review Quarterly* (Summer 1994).

"Net Profit or Loss." *Security Awareness News,* October 1995.

Panettieri, Joseph C. "Are Your Computers Safe?" *Information Week,* 28 November 1994.

Plate, Thomas and William Tuohy. "John Major; Even Under Fire, Britain's Prime Minister Holds His Own." *Los Angeles Times,* 20 June 1993.

Pollard, Neal. "Computer Terrorism." Address. 1995 International Information Warfare Conference, Arlington, Va., 7 September 1995.

RAND. *The Day After . . . in Cyberspace.* Santa Monica, Calif.: RAND, 1995.

———. *Strategic Information Warfare: A New Face of War.* Washington, D.C.: RAND, 1995.

Ronfeldt, David. *Cyberocracy, Cyberspace and Cyberology: Political Effects of the Information Revolution.* Santa Monica, Calif.: RAND, 1991.

Rosen, Stephen. *Winning the Next War: Innovation and the Modern Military.* Ithaca, N.Y.: Cornell University Press, 1991.

Ryan, Julie J. C. H. "Information Warfare: A Conceptual Framework." Lecture. Seminar on Intelligence and Command and Control. Center for Information Policy Research, Harvard University. Cambridge, Mass., 7 March 1996.

Sandberg, Jared. "GE Says Computers Linked to Internet Were Infiltrated." *The Wall Street Journal,* 28 November 1994.

Schwartau, Winn. *Information Warfare: Chaos on the Electronic Super Highway.* New York: Thunder's Mouth Press, 1994.

Schweizer, Peter. *Friendly Spies: How America's Allies Are Using Economic Espionage to Steal Our Secrets.* New York: Atlantic Monthly Press, 1993.

Science Applications International Corporation (SAIC). *Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance.* Washington, D.C.: SAIC, 1995.

———. *Planning Considerations for Defensive Information Warfare.* Washington, D.C.: SAIC, 16 December 1993.

Sikorovsky, Elizabeth. "Internet Break-ins Compromise NASA Data." *Federal Computer Week,* 19 December 1994.

Smith, James M. "Logic Flaw is the Culprit in Computer Mugging." *Government Computer News,* 7 November 1994.

Soft Kill. CD-ROM. Xiphas, 1993.

Steele, Robert. "The Military Perspective on Information Warfare: Apocalypse Now." Address. Second International Conference on Information Warfare. Montreal, Canada, 19 January 1995.

Stein, George. "Information Warfare." *Airpower Journal* 9, no. 1 (Spring 1995).

Strassmann, Paul A. "Defending the Military Infrastructure." Address. Washington, D.C.: National Defense University, 11 March 1996.

———. "Risk-Free Access Into the Global Information Infrastructure Via Anonymous Re-Mailers," Symposium on the Global Information Infrastructure. Kennedy School of Government, Harvard University, Cambridge, Mass., 28–30 January 1996.

Summers, Harry G. *On Strategy: A Critical Analysis of the Vietnam War.* Novato, Calif.: Presidio Press, 1982.

Thompson, Mark. "If War Comes Home." *Time,* 25 August 1995.

Thurow, Lester. *Head to Head: The Coming Economic Battle Among Japan, Europe and America.* New York: Morrow, 1992.

Toffler, Alvin, and Heidi. *War and Anti-War: Survival at the Dawn of the Twenty-First Century.* Boston: Little, Brown and Co., 1993.

United States. Department of Defense. *1994 Defense Science Board Summer Study on Information Architecture for the Battlefield.* Washington, D.C.: Defense Science Board, 1994.

———. General Accounting Office. *Information Superhighway: An Overview of Technology Challenges.* Washington, D.C.: GPO, 23 January 1995.

———. National Communications System. *An Assessment of Risk to the Security of Public Networks.* Washington, D.C.: National Communications System, December 1995.

———. ———. *The Electronic Intrusion Threat to National Security and Emergency Preparedness Telecommunications: An Awareness Document.* Arlington, Va.: National Communications System, December 1994.

———. Navy. *Space and Electronic Warfare: A Navy Policy Paper on A New Warfare Area.* Washington, D.C.: GPO, 1992.

———. Senate. Foreign Relations Committee. *Hearings on the Subcommittee on Terrorism, Narcotics and International Operations.* 103d Cong., 2d sess. Washington, D.C.: GPO, 20–21 April 1994.

———. White House. *National Security Strategy of the United States.* Washington, D.C.: GPO, August 1991.

Villacres, Edward J., and Christopher Bassford. "Reclaiming the Clausewitzian Trinity." *Parameters,* Carlisle, Pa.: US Army War College, August 1995.

Waller, Douglas. "Onward Cyber Soldiers." *Time,* 21 August 1995.

Warden, John A., III. "The Enemy as a System." *Airpower Journal,* Spring 1995.

*U.S. GOVERNMENT PRINTING OFFICE:1998-636-926/60233