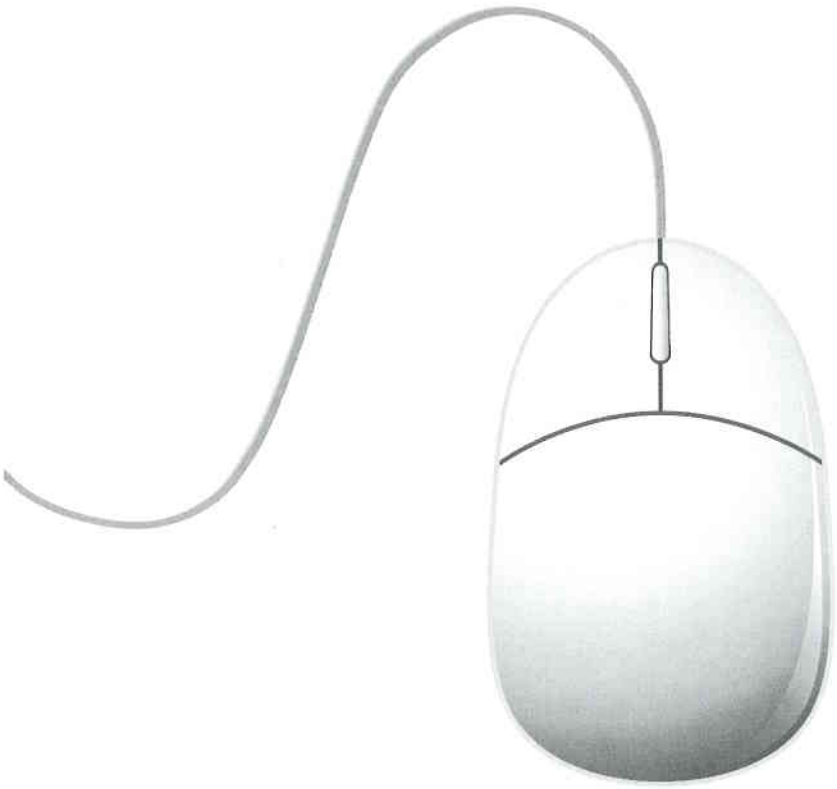
ISSN 1345-0093

COM

愛知大学情報メディアセンター紀要

Vol.16/No.1 2005.September



情報メディアセンター利用案内

◇サービス時間〈月～土曜日〉

（都合により変更する場合があります。掲示をご覧下さい。）

車道校舎

期間		K701、K802、K804	メディアゾーン
通常講義 定期試験		講義利用のみ	9：00 ～ 22：00
補講 集中講義	試験前		9：00 ～ 19：00
	試験後		
上記以外			

豊橋校舎

期間		420教室 （オープンアクセスルーム）	メディアゾーン （図書館）※1	413教室・421教室・ 423教室・424教室・ 514教室・523教室
通常講義 定期試験		9：10 ～ 21：00	9：10 ～ 21：00	講義利用のみ （420 教室の状況により一般利用できます。）
補講 集中講義	試験前	9：10 ～ 21：00	9：10 ～ 21：00	
	試験後	9：10 ～ 19：00	9：10 ～ 18：30	
上記以外		9：10 ～ 19：00	9：10 ～ 18：30	

※1 メディアゾーンは、豊橋図書館の運用日程に準じます。

名古屋校舎

期間		第1･2･3実習室	マルチメディア教室 （中央教室棟）	E201教室 E202教室 （東教室棟）	メディアゾーン （図書館棟2F）※2
通常講義 定期試験		9：10～19：50	講義利用のみ	9：10～18：10 （E202教室は講義利用のみ）	9：10～20：00
補講 集中講義	試験前				
	試験後	9：10～19：00			
上記以外				休み期間は原則閉室	9：10～19：00

※2 メディアゾーンは、名古屋図書館の運用日程に準じます。

■センター閉室日 ／ 日曜日・祝日・夏期休暇期間・年末年始・創立記念日（11/15）・入試期間

◇メールリストサーバ

アドレス	list@aichi-u.ac.jp
subject の記述	meibo（教員）, meiboj（職員）
郵送される資料	電子メールアドレス

はじめに

情報メディアセンター長　龍　昌治

大学で情報処理教育が行われるようになって、久しい。本学においても、情報処理センターが設置され、汎用機を用いたコンピュータ教育・プログラミング教育の黎明期からはじまり、幾度かのシステム更新やカリキュラム変更をへて、現在の情報リテラシー教育へと引き継がれています。この間、使用される情報機器は、汎用機とその専用端末という構成から、ローカルエリアネットワークとパーソナルコンピュータへと変化しています。対象となる学生も、計算機科学やプログラミングを学ぶ一部の学生から、いわゆる文科系の全学生へと大きく拡大してきました。一部の学生を対象にした汎用機を用いたコンピュータ教育を、第1期情報教育とよぶなら、第2期情報教育は、全学生向けのパソコンを用いたパソコン操作教育といえるでしょう。

2003 年度から実施されている高等学校等の情報教育は、「情報活用の実践力」「情報の科学的理解」「情報社会への参画」の 3 要素で構成されています。このカリキュラムで学んだ学生たちが、大学に入学する 2006 年度に向けて、各大学では情報教育カリキュラムの改訂が計画されています。大学における第3期情報教育ともいえる今回のカリキュラム改訂は、単なる操作教育ではなく、真の意味での情報リテラシー教育への転換が求められています。すなわち、情報科学や技術を理解しつつ、課題発見や問題解決のツールとして、主体的に情報を扱える能力の育成です。次世代の社会を構成する若者たちにとって、欠くことのできない能力のひとつでしょう。

大学における情報教育の中心をになってきた、情報メディアセンターの果たすべき役割や機能も、少しずつ変化が必要です。単なるハコモノとしてではなく、学生や教職員にとっての活動の中心であり、HUB としての機能が求められています。このセンター機能は、ユーザの皆さんが求めてこそ、価値を発揮するものです。“使える”センターとして、なお一層、学生や教職員の皆さんのご利用・ご協力をお願いいたします。

目　　次

1．論文

インターネット社会の安全性を確保するための国際的取り組みに関する考察

Consideration of International Effort for Security on the Internet

宮田 裕之，土橋 喜
Hiroyuki Miyata,　Konomu Dobashi

愛知大学現代中国学部
Faculty of Modern Chinese Studies Aichi University

目　次

はじめに

情報化社会の発展に伴い，現代社会の基盤を支える多くの分野において，業務の効率性や生産性を向上させるためにコンピュータ・システムが導入されている．一般企業や政府関係などのさまざまな日常的な業務だけでなく，電気・ガス・公共交通機関などの重要なインフラストラクチャにおける運用や維持管理にもコンピュータ・システムは不可欠になっている．先進国をはじめとした多くの国々においてコンピュータ・ネットワークは産業や社会を支える重要な社会基盤であり，故障や操作ミスなどによりこれらのコンピュータ・システムが停止するような異常な事態が発生すると，社会に対してさまざまな影響を与えかねない．

このようなことからコンピュータ・システムの障害は，一旦犯罪に悪用されると人々の社会生活に対して大きな悪影響を及ぼす危険性があることが指摘される．近年ではこれらのコンピュータに依存した情報化社会の弱点を狙い，社会を混乱させようとくわだてるサイバーテロの発生が懸念されはじめている．さらにコンピュータを利用したサイバー戦争を重要な国家戦略として位置づけている国もある．ダン・バートンの著書によれば，アメリカ，ロシア，インド，イスラエルなどでは，サイバー戦争を前提としたデジタル兵器の開発を行っているといわれている[1].

新聞などのメディアによればソフトウェアの欠陥であるセキュリティホールを狙い，官公庁や企業のコンピュータに悪意を持って不正侵入し，データの改竄やシステムを停止させるなどのクラッキングが最近も頻繁に発生しており，実際に企業の業務が停止に追い込まれる事態も起きている[2]．コンピュータに危害を与えるコンピュータウイルスの流布も，年々件数が増加し被害も増加傾向にあり，国際的に深刻な社会問題となっている．このようなコンピュータ犯罪による被害は，経済的に大きな損失を与えるだけでなく，人々が利用する日常の通信を麻痺させるなど，社会を混乱に陥れることがしばしばである．

国家や企業などのコンピュータに不正アクセスを行い，それらの組織に対して何らかの悪影響を与えようとするサイバー攻撃は，ネットワークを使用すれば場所を問わずどこからでも行うことができる特徴を持っている．さらにインターネットでは通信経路が常に一定ではないため，攻撃者を特定することを困難にしている．サイバー攻撃を事前に防ぎ，攻撃者の所在を特定するためには．国内のみならず海外においても幅広い情報収集活動が必要となり，場合によっては多国間で捜査協力を行い，捜査情報を共有する必要もある．

しかし現時点ではサイバーセキュリティ関連の法制度や捜査体制は十分に整備されているとは言いがたく，攻撃者を特定したり摘発したりすることが困難な状況にある．これらのサイバー犯罪の発生を防ぎ，犯罪者を取り締まることを目的とした国際的な法律の制定や捜査機関の設立が急務とされている．

現在多くの国々においてサイバーテロあるいはサイバー攻撃への対策が重要視され，法律・条約の制定や専門の捜査機関の設置がすすめられている．サイバーテロやサイバー攻撃を取り締まる法制度が整備されるなかで，他方ではコンピュータ・ネットワーク上で送受信される情報を監視するシステムが設けられるなど，ネットワーク上で行われる不正な活動を監視しようとする動きもある．だがそれらの監視システムが整備されることによって，本来守られるべき通信の自由と秘密および個人のプライバシーを侵害する危険性も高まることが問題点として指摘されている．

本論は小規模な不正アクセスによるサイバー攻撃だけでなく，被害が広範囲に広がるサイバーテロやサイバー戦争などを防ぐため，情報セキュリティを確立するための国際的な取り組みについてまとめた．さらにサイバーテロの発生を防ぐため，それらを取り締まるために制定された法律や制度についても取り上げ，ネットワーク監視システムなどの弊害や，それらから保護されるべき市民の権利について論じる．

第1章　現代社会とサイバーテロの脅威

1．テロリズムの変化

2001 年 9 月 11 日米国ニューヨークのマンハッタンにある世界貿易センタービルで発生した旅客機突入によるビル崩壊事件以降，テロという言葉が盛んに使われている．この事件以降マスコミの報道や政府の見解などでは，テロという言葉を無差別な殺人を伴う破壊活動を指すものとして使用されることが多くなった．テロまたはテロリズムの本来の意味は，意図的・計画的に不法な手段によって政治的な目的を達成するため，暗殺や暴行などの手段を認める主張であり，またそれに基づいて実際に暴力的な行動を起こすことである．テロの結果として一般市民を巻き添えにしたり，人々に恐怖感を与えることにもなる．米連邦捜査局(FBI)国家インフラストラクチャ保護センター(NIPC: National Infrastructure Protection Center)の報告では，「テロリストの組織は，通常社会の尊厳となる象徴的なターゲットを攻撃する．そうしたシンボルへの攻撃が成功すれば，市民はそれまで安全だと信じていた社会から個人的に切り離され，政府に対して不安感を抱くようになる．このようなテロリストの破壊的な行動によって，市民を守るべきはずの政府の能力に対して，人々が疑問を抱くようになる．このようなときに市民は他者からの影響に最も左右されやすくなる」と指摘している．言い換えれば人々に恐怖心を植え付けることにより，暗殺や暴行などの不法な手段によって，政治的な目的を達成しようとすることがテロリズムの本質的な目的であるといえる[3].

2．サイバーテロとサイバー攻撃

サイバーテロ(cyberterrorism)とは，一般的には国家や社会基盤を混乱させる目的で，コンピュータ・システムへ不正に侵入し，破壊活動を行うことを指す比較的新しい造語である．現代用語の基礎知識には「コンピュータ・ネットワークを通して国防，治安をはじめ通信・交通など，国民生活を支える重要インフラのコンピュータ・システムに侵入し，国家や社会の重要な基盤を機能不全に陥れることを目的としたテロ行為」であると解説されている．

また NIPC の報告には，「コンピュータと通信を悪用することによる犯罪行為であり，各種のサービスを破壊または停止させることにより，特定地域の住民に混乱と不安をもたらし，恐怖を生み出す犯罪行為である」とサイバーテロをより広く定義している[4]．さらにこの定義に付随して，テロリズムは伝統的な物理的破壊行為を意味するものであったが，最近の情報化時代ではサイバーテロの定義について，より実態を反映したものに再定義するべきであると主張している．これまでは政府機関や社会のインフラを担うコンピュータ・システムを破壊したり，緊急通報システム，電話サービス，銀行システム，インターネットなどの重要なサービスを管理するコンピュータ・システムを破壊したりして，市民の社会生活を混乱させるテロリズムなどがサイバーテロの代表と見なされていた．

これに対してサイバー攻撃(cyberattack)は，「インターネット経由で他のコンピュータに不正アクセスを行い，相手の国家や企業にダメージを与えようとする行動のことである．実際に行なう内容は不正アクセスとまったく同じだが，政治的な意図を持って行われる不正アクセスがサイバー攻撃と呼ばれる傾向にある（IT 用語辞典 e-words）」．

サイバー攻撃の手法は多数あるが，その攻撃となる対象により大きく分けて２つのタイプがあるといわれている．ひとつは攻撃したい組織内の特定のサーバーを目標と定め，そのサーバーにダメージを与えて運用を停止させることを目的に，様々な不正アクセスによる攻撃を加える．これはターゲットになる企業や国家などの組織が特定されており，目標とされる組織に対する恨みなどから嫌がらせをするために行われる．あとひとつは目標となるサーバーを特定して行うものではなく，主に OS などのソフトウエアが持つセキュリティホールを狙い，混乱の原因となるデータやウイルスを無差別に送りつけるものである．主に社会全体を混乱させるのが目的で行われることが多い．

ここでは被害が特定の企業や組織に限定され，政治的な意図の少ないものをサイバー攻撃とみなし，被害が多数に及び多分に政治的な目的を持ち，地域の住民に混乱と不安をもたらして恐怖感を与えるようなものをサイバーテロと考えることにする．

3．サイバーテロの脅威

サイバーテロに対しては，被害が甚大になった場合を想定して十分な警戒が必要であるという意見がある．これに対して社会の重要インフラなどのシステムは，たとえ不正侵入に成功してシステムをコントロールできたとしても，さまざまな防御体制が用意されており，社会が破局的な状態に陥ることを防いでいる．不正侵入やクラッキングよりも，爆弾を仕掛けるほうが簡単であるといわれ，サイバーテロを過大評価すべきではないという意見もある．このような意見がある中で，物理的テロとサイバーテロの同時実行や，原子力発電などに代表される重要インフラと通信などの情報インフラへの同時多発テロの実行などは，十分な対策を考えておく必要がある．しかしサイバーテロに対する恐怖感を必要以上にあおると社会的混乱を引き起こす危険性もあるため，この点で充分注意することが重要である[31].

今後はサイバーテロだけで犯罪を行うのではなく，従来の武力や爆弾などによるテロ攻撃と組み合わせ，テロの効果を倍加させることを目的として行われることも危惧されるようになった．コンピュータを使いネットワークから侵入して破壊行為などを行うだけがサイバーテロではなく，爆発物などにより直接コンピュータセンターを物理的に破壊する行為も，サイバーテロと同様かそれ以上の被害をもたらす．爆発物などを使用する破壊活動は以前からテロリストが用いてきた伝統的な手法である．このような攻撃方法ではコンピュータに関する専門的な知識は不要であり，ネットワークから相手のコンピュータ・システムへ侵入するサイバー攻撃より，物理的な被害をも同時に伴う分より多くの被害を与えることが想定される．

サイバーテロは攻撃対象がコンピュータ・システムであること以外は伝統的なテロ行為と同じであるが，今後のサイバーテロは従来のテロリズムが持つ側面をも併せ持つといえる．わずかな資金で甚大な被害を与える可能性があるサイバー攻撃に関心を抱く人々はテロリストだけではない．個人をはじめ国家や民間組織，または既成の社会から正統的とはみなされない宗教的集団であるカルト集団まで様々であり，サイバーテロの目的は軽いいたずらから恨みばらしまで含まれ多種多様である．

これまでのところサイバーテロによる直接的な死傷者は出ていないといわれている．だが死傷者が出ていないからさほど脅威ではないと結論を急ぐことはできない．安保克也らによればネットワークからの直接的な攻撃で人を死傷させることは難しいが，間接的な攻撃では死傷者が発生する可能性もある．サイバーテロとして狙われる対象は軍事施設だけではなく，電気やガスなどの重要なライフラインも攻撃対象にされるため，一般市民を巻き添えにした無差別テロに発展する可能性もあるといわれる[6]．サイバーテロは社会に政情不安をもたらすことを目的としているため，社会生活と密着したライフラインへの攻撃は無差別的な要素を持つとともに，施設自体の攻撃は二次的な目的でしかない．現に中東のイスラエルやパレスチナ自治区をはじめとした世界の紛争地域では，市民の日常生活と結びついた公共交通機関のバスが爆破されるテロがたびたび発生しており，市民に多大な恐怖感を与えているのである．

以下にダン・バードンの著書を参考に，現段階で想定される重要インフラと関連させたサイバーテロの被害例を挙げてみたい[1]．サイバー攻撃によって航空管制システムのコンピュータを破壊し航空管制を麻痺させた場合，航空機同士の衝突事故が起こる危険性が高くなる．今後も航空機は増加するため，特に混雑する飛行場近辺の上空や離着陸時における事故の危険性が高まるといえる．発電所の発電量や電気の供給を管理するコンピュータを破壊して電力の供給に障害を与えれば，大部分が電気によって支えられている現代の社会生活は麻痺状態になり，人々の生活に混乱をもたらすことが予想される．貯水量の多い大規模なダムの水門を予告もなく突然開いて放水させ，河川の水量を増やして下流にある都市を浸水させることも考えられる．

なかでもサイバー攻撃に関するケースで最も恐ろしいものは，原子力関連施設への攻撃である．原子力発電所などの原子力技術関連施設はコンピュータによって管理されている．そのため原子力発電を行う際に使用される核融合炉の炉心温度を管理するコンピュータを悪意に操作して炉心温度を上昇させた場合，1986 年にウクライナのチェルノブイリ発電所で発生した原子炉融解事故に類似した事故を人為的に引き起こすことができる．放射能汚染が国境を越えて蔓延すれば，地球規模での問題にもなりかねず，その被害は計り知れないものがある．

さらにサイバー攻撃だけでテロを実行するよりも，生物・化学兵器の利用や爆弾テロなどと同時攻撃を加え，電話の 110 番や 119 番などに代表される緊急通報システムの破壊と組み合わせることにより，負傷者の救助を遅らせ死傷者の数を増やすなど，従来の攻撃手段の効果を高めるものとして利用される

危険性も否定できない．これまで見てきたように社会のあらゆる場面でコンピュータが使用されている現代社会では，サイバーテロの脅威に対して防衛策を実施しなければならない．先進国ほどコンピュータ・システムへの依存度が高く，サイバーテロによる被害は現代社会の崩壊をもたらしかねない危険性を持っている[7]．安保克也らによれば米国ではすでにサイバー攻撃による被害件数は 250 万件以上であり，その被害総額は国家予算規模に上るのではないかといわれている[8]．そのため米国ではサイバーテロによる脅威は．ミサイルや核兵器，生物・化学兵器などによる大量殺戮兵器の拡散と同程度に重大であるとみなす軍事専門家も存在する．

核兵器の開発には科学技術の知識に基づいた高度な技術力が必要であるが，その破壊力は極めて甚大であり，北朝鮮の核開発には世界中が注目した．これに対して生物・化学兵器は少ない人数でも使い方次第で大きな被害を与えうる危険性があることから，「貧者の核兵器」と呼ばれる．生物・化学兵器は製造コストが核兵器に比べて安く，僅かな量でも核兵器に相当する人的被害を与えることができるからである．これらの生物・化学兵器と同様にサイバー攻撃は，わずかな資金と労力で大きな被害を与えうる危険性を持つと見なされており．テロリストらがコンピュータを有用な兵器として注目し研究しても不思議ではない．このようなことから宮脇はサイバーテロを「第三の貧者の核兵器」として警戒すべきであると指摘している[5]．

(1) サイバーNGO の出現

環境保護や原子力発電の廃止あるいは野生動物保護など政治的な主張を掲げる NGO が，関連する国際会議の開催や国際条約の締結に合わせ，問題の当事国となっている政府機関や企業のウェブサイトに対し，政治的な抗議活動の一環として不正アクセスなどによるサイバー攻撃を行うことがある．このように政府機関や大企業のコンピュータに対し，意見を同じくする者が集団となってサイバー攻撃を仕掛ける非政府組織を，宮脇磊介は「サイバーNGO」と呼んでいる．これらの集団も攻撃対象となる組織や個人に被害を与える危険性があることから，インターネット上のテロリストと同様に問題があると指摘している[9]．サイバーNGO の中には多数の参加者を集め，議員や政治団体などに電子メールで抗議文を送ったり，インターネット上に公開されている掲示板やメーリングリストなど利用して自分達の意見を多量に書き込んだりすることもある．

(2) ハクティビズムの台頭

ハクティビズムとは，攻撃者を意味する「ハッカー」と政治的行動主義を意味する「アクティビズム」を合成した造語である[10]．政治思想や価値観あるいは宗教観において自己の確立した主張を持ち，自己の思想や宗教観と敵対する組織や団体に対し，インターネット上で様々な攻撃を行っている．イスラエル，パレスチナ，インド，パキスタンなどの国々で多く見られ，最近では中国などにも類似の攻撃を行う集団が存在していることが確認されている．日本の靖国神社や官公庁のサーバーなどはその攻撃対象となった．これらハクティビストの活動は年々活発化すると予想されており，ハクティビズムはインターネット上で行われるゲリラ的な政治活動の現われとみなされる．敵対するウエブサーバーに不正侵入して内容を書き換えることにより,政治的なメッセージの宣伝を行ったり，サーバーが処理しきれないほどのデータを送りつける分散型サービス拒否攻撃（DDoS 攻撃，Distributed Denial of Service）を行うことも多い．近年では新興宗教団体などの組織もサイバーテロに興味を示している[11]といわれて

おり，現実にカルト集団として中国政府に一切の活動を禁じられた法輪功が，2002 年 6 月テレビ用通信衛星の送受信機に侵入し，何百万人もの視聴者へ政治的な宣伝メッセージを送る事件が発生した[12].
この事件の発生は民間団体であってもサイバーテロの実行が可能なことを実証する結果になった.

(3)歴史教科書問題とサイバーデモ

サイバーデモとは，インターネット上で主張を同じくする賛同者が多数参加して，政治的な目的を実現するための統一行動を行い，特定のウエブサイトなどに対して不正アクセスなどを行うものと解されている．日本においては 2001 年に歴史教科書問題が起きた際に最初のサイバーデモが発生した．新しい歴史教科書を作る会によって作成された教科書が公表されると，2000 年から 2001 年にかけて日本を含むアジア諸国で社会問題となった. これが首相の靖国神社参拝とあいまって中国・韓国などの近隣諸国と深刻な外交問題に発展していた．これら日本の歴史教科書問題に関する抗議活動として 2001 年 3 月，文部科学省，自由民主党，産経新聞社など合計 6 ヶ所のウェブサイトが中国や韓国などから攻撃された．この事件では極めて多数の賛同者が，予め定められた時刻に攻撃対象のサーバーに対し同時にアクセスを行う攻撃が行われ，サーバーの処理能力を超える過大な負荷により，ウェブサイトが提供する正常なサービスを停止させるなどの被害を与えた(図 1).

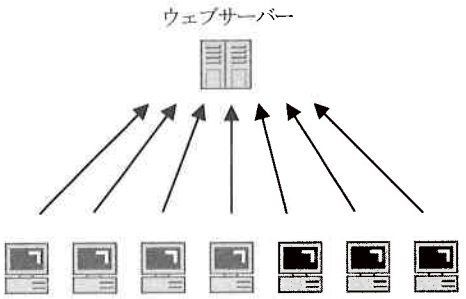


図 1）ウェブサーバー攻撃の概略図

この事件の直前には同時アクセスの準備として，インターネット上で賛同者を募り，特定のサイトを攻撃するために作られた専用ソフトが不特定多数の人々に配付されていた．この専用ソフトを使用すれば画面をクリックだけで，コンピュータに関する高度な知識がない者でも，簡単に攻撃に参加することができる仕組みになっていた．これによって多くの賛同者が容易に攻撃に参加することができたため被害を大きくした．また一時的ではあるが同じ意見を持つ賛同者が，インターネット上で一つの仮想的な組織を結成して攻撃に参加する統一行動が見られた．これらの点からこの事件はインターネット上で行われる「サイバーデモ」の一種であったと見なされている．この事件では近隣諸国からの DDoS 攻撃やクラッキングが行われたことが明らかであった．しかし日本以外からの国から攻撃を行っているため，当時の日本の法律で裁くことは困難であり，誰一人として逮捕されることはなかった.

同様のサイバーデモは，2005 年 4 月に中国の上海などいくつかの主要都市で反日デモが発生した際にも起きており，中国の日本大使館のウエブサーバーに大量の不正アクセスが行われ，接続障害を起こし