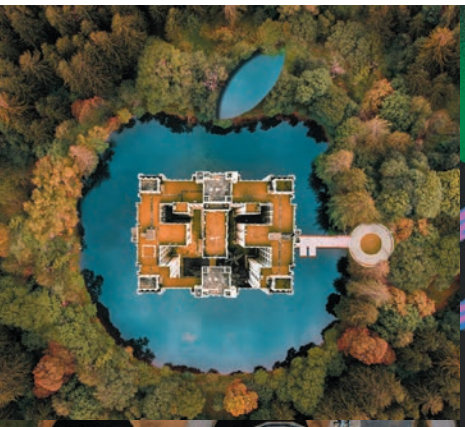
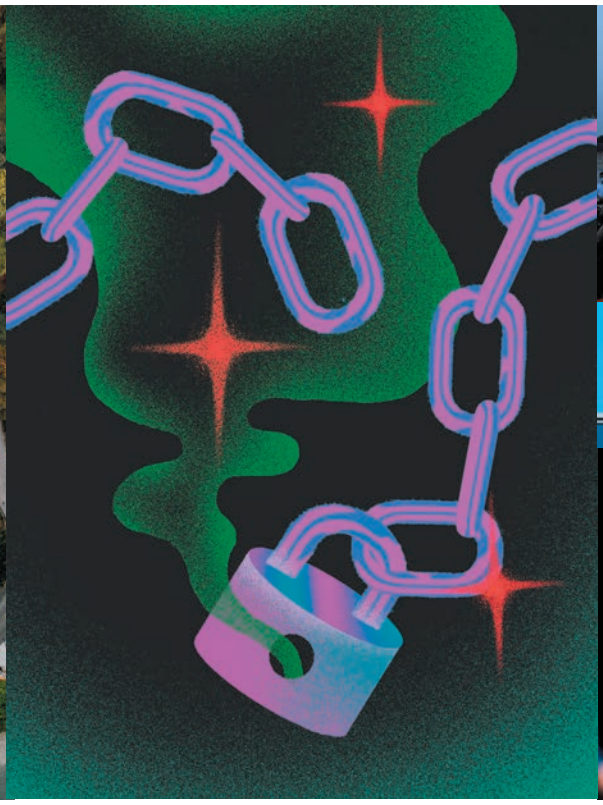
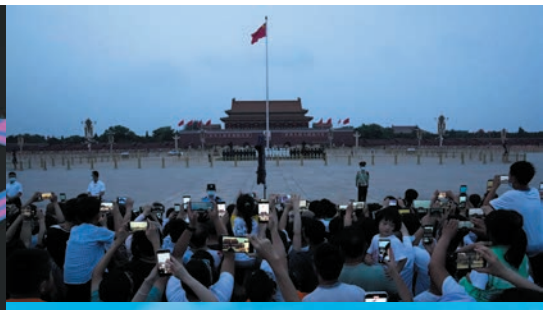
MIT Technology Review
Published by KADOKAWA / ASCII

Cyberwarfare

静かなる国際紛争

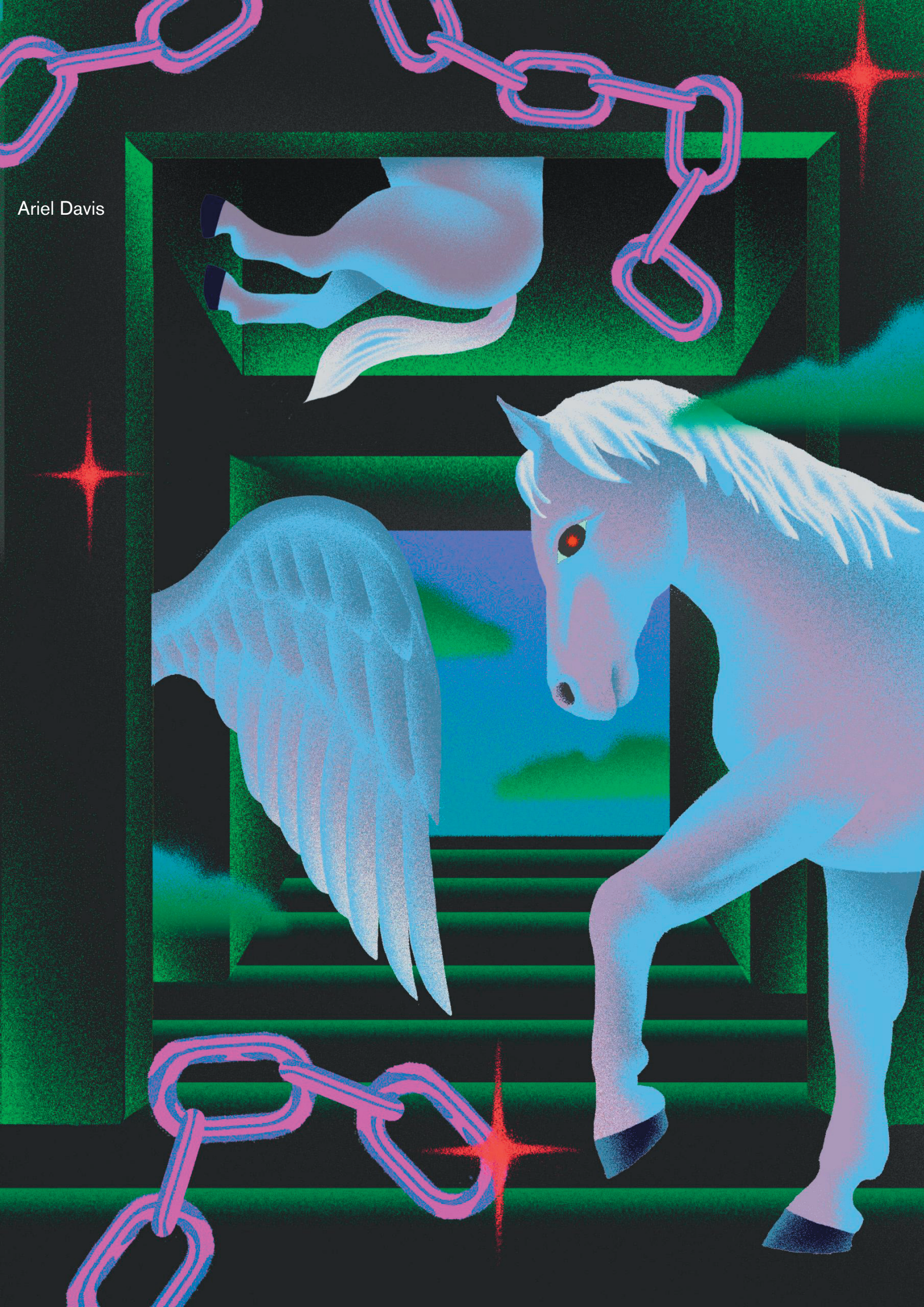






サイバー空間を舞台に、静かなる国際紛争が広がっている。スマートフォンに潜むスパイウェア、インフラ企業を事業停止に追い込むランサムウェア、ソフトウェアの脆弱性を利用して企業内ネットワークを乗っ取るゼロデイ攻撃などの手段によって、一般市民の人命や経済が脅かされているのだ。背景には、ビジネスとしてスパイウェアを販売するソフトウェア企業や、政府の支援を受けたハッキング集団の躍進がある。どのような攻撃、どのような防御が繰り広げられているのか。その一端を明らかにした記事をまとめた。

CONTENTS


Ariel Davis

現代の「死の商人」、謎のイスラエル企業 NSO グループの正体

by Patrick Howell O'Neill

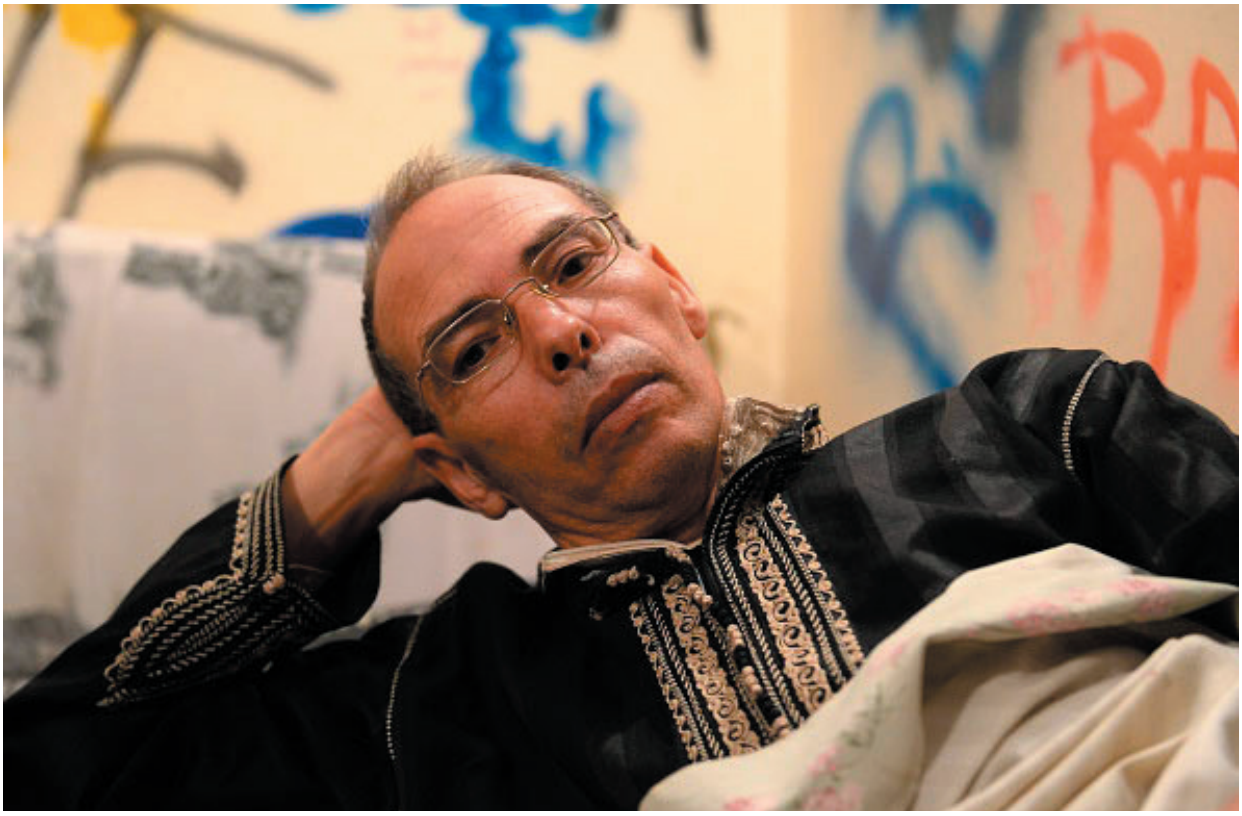
サウジアラビアのジャーナリスト殺害で、一躍その悪名が高まった世界的なスパイウェア企業は、不透明な企業運営を改めるために動き出していた。だが、企業側が主張する不正利用を防ぐ仕組みと実態との間には大きな乖離があり、自主規制だけでは不十分だ。

マーティ・モンジブはゆっくりと話す。まるで、会話を聞かれていることを知っているかのようだ。

その日はモンジブの58回目の誕生日だったが、彼の声におめでたい雰囲気はあまり感じられなかった。「監視は地獄です」。モンジブは言う。「本当に辛いものです。生活の中でやること、なすことすべてが管理されています」。

モロッコのラバトにあるムハンマド5世大学（University of Mohammed V）の歴史学の教授であるモンジブは、自分の人生が変わった2017年のあの日のことを鮮明に覚えている。それまで公の場で激しく政府を批判してきたモンジブ教授は、国家安全保障を危険にさらしたとして政府から告発された。法廷の外で座っていたとき、突然アイフォーン（iPhone）に知らない番号からショート・メッセージが立て続けに送られてきた。そこには卑猥なニュース、嘆願書、さらにはブラック・フライデーのセール広告へのリンクが含まれていた。

1カ月後、モロッコ王室とつながりの深い一般向けの全国版ニュースサイトに、モンジブ教授の反逆を告発する記事が掲載された。モンジブ教授は攻撃されることに慣れていたとはいえ、今や、嫌がらせをする人たちは彼のことを何でも知っているようだった。別の記事には、モンジブ教授が参加する予定だった民主化運動に関する情報が掲載されていた。しかし、彼は誰にも参加を話して



モロッコの大学教授で言論の自由を求める活動家でもあるマーティ・モンジブは、
政府に数年間監視されている。彼は「監視は地獄です」という（写真：GETTY）

いなかった。「（モンジブ教授には）秘密にしておけるものは何もない」とさえ書いている記事もあった。

モンジブ教授はハッキングされていたのだ。立て続けにアイフォーンに送られてきたショート・メッセージは、すべてあるWebサイトにつながっていた。セキュリティ研究者によると、このサイトは、アクセスしてきた端末に、世界で最も悪名高いスパイウェア「ペガサス（Pegasus）」を感染させるルアーのような役割を果たす。

ペガサスは、秘密のベールに包まれたイスラエルの10億ドル規模の監視企業、NSOグループ（NSO Group）の大ヒット製品で、世界中の司法当局や情報機関に販売されている。これらの組織がターゲットとなる人を選び、その人の携帯電話をスパイウェアに感染させ、デバイスを乗っ取るのに使用する。いったんペガサスに感染すれば、その携帯電話はもうその人自身のものではなくなってしまう。

NSOは、武器商人が従来の武器を販売するのと同じように、テロリストや犯罪者を探し回るのに欠かせないものとしてペガサスを販売してい

る。モバイルデバイスと強力な暗号化の時代、こうした「合法的なハッキング」は、司法当局がデータにアクセスしなければならない場合に使う、公共の安全のための強力なツールとして登場した。NSOは、顧客の大多数が欧州の民主主義国だと主張しているが、顧客リストは公開しておらず、利用国も沈黙を守っているため、事実かどうかは検証されていない。

だがモンジブ教授の場合は、ペガサスが弾圧の道具として使われた数多くの例の1つだ。ペガサスが関係している事件の中には、サウジアラビアのジャーナリスト、ジャーマル・カショギ殺害事件、メキシコで政治改革を推し進める科学者や活動家や、スペインのカタルーニャ州分離独立派の政治家に対する政府の監視などがある。メキシコとスペインの当局は、ペガサスを使用した対立相手の監視は否定しているが、それを裏付ける技術的な根拠があるとして批判されている。

ペガサスが悪用された証拠の1つが、2019年10月、カリフォルニア州でペガサスがワッツアップ（WhatsApp）のインフラを操作して1400台以上の携帯電話を感染させたとして、ワッツアップとその親会社のフェイスブックが起こした訴訟だ。裁判書類によると、フェイスブックの調査担当者はターゲットの中に人権擁護者、ジャーナリスト、著名人が100人以上いるのを発見した。電話がかかってくるたびに、ワッツアップのインフラを介して悪意のあるコードを送信し、受信者の携帯電話にNSOが所有するサーバーからスパイウェアをダウンロードさせていたことも分かった。ワッツアップが主張するように、これらは米国の法律に違反する行為だ。

NSOは政府が使用するテクノロジーの生みの親ではあるが、NSOが直接誰かを攻撃しているのではなく、責任は負えないというのがNSOの基本的な主張だ。

NSOは長年このような批判に対して、沈黙を続けている。NSOは事業の大部分がイスラエルの国家機密だと主張し、運用や顧客、悪用予防条項といった重要な詳細をほとんど公表していない。

だが現在、NSO には変化の兆しが見られる。2019 年、未公開株式投資会社が所有していた NSO は、創業者と別の未公開株式投資会社ノバルピナー(Novalpina)に 10 億ドルで売却された。新しいオーナーは斬新な戦略を決定した。表の世界に出ることにしたのだ。有名広告会社と契約し、新しい人権政策、そして新しい独自のガバナンス文書を作成した。さらに新型コロナウイルス感染症（COVID-19）追跡システムの「フレミング(Fleming)」、安全上の脅威とみなしたドローンをハッキングできる「イクリプス（Eclipse)」といった製品もアピールするようになった。

私は数カ月にわたって NSO の幹部に話を聞き、会社の仕組みや、自社ツールの使用による人権侵害を防ぐために何をしているのかを知ろうとした。そして、NSO を民主主義的価値に対する脅威とみなす批評家たち、ハッキング・ビジネスの規制強化を求める人々、そして現在 NSO の管理責任を負うイスラエル規制当局も取材した。NSO の幹部は、NSO の未来とポリシー、問題に対処するための手順について語り、ペガサスなどのツールを販売した機関との関係を詳述した文書を公開した。そこで私が見つけたのは、業界全体の基盤を脅かす新しい緻密な調査に悪戦苦闘しながらも繁盛している武器商人、NSO の姿だった（NSO 社内では従業員もペガサスが正真正銘の武器だと認識している)。

「難しい仕事」

シュムエル・サンレイは、法務部長として NSO で働き始めた初日から、次から次へと国際的な問題に直面してきた。ワッツアップから訴訟を起こされたわずか数日後に入社したサンレイ部長のデスクの上には、別の法的問題が山積みになっていた。どれも同社を非難するものばかり。つまり、悪用される可能性のある NSO のハッキング・ツールは、金持ちの独裁政権に販売され、乱用されてもほとんど何の責任も負わないことについてだ。

前職が大手武器メーカーの副社長だったサンレイ部長は、秘密保持と論争の経験が豊富だ。何度

か話しをするうちに、打ち解けてきたサンレイ部長は、オーナーから NSO の社風や運営を変えるよう指示されており、透明性を高め、人権侵害が起きないようにしていると話してくれた。だが一方でサンレイ部長は、秘密保持のせいで批評家たちに反論できないことに明らかに苛立っていた。

「難しい仕事なんです」。テルアビブ北部ヘルツリーヤにある NSO 本社からの電話でサンレイ部長は話した。「我々はツールの力を理解しているし、ツールを悪用された場合の影響も理解しています。我々は、正しいことをしようとしています。政府、情報機関、機密性、運用上の必要性、運用の制限への対処が現実的な課題です。当社は企業による人権侵害の典型例ではありません。なぜなら NSO は実際にシステムを運用をしておらず、関わってもいないからです。それでも顧客に悪用される、現実的なリスクは理解しています。我々は適切なバランスを見つけようとしています」。

これは NSO の基本的な主張を裏付けるものであり、武器製造業者がよく使う主張でもある。NSO は政府が使うテクノロジーの生みの親だが、NSO 自体が誰かを攻撃しているのではなく、責任は負えないというのだ。

サンレイ部長によると、それでも不適切な人がアクセスできないように、複数の予防策は準備しているという。

慎重に販売している

他の国々と同じくイスラエルには輸出規制があり、武器製造業者はライセンスの取得が必要で、政府の監視下に置かれる。さらにサンレイ部長は、NSO は独自のデュー・デリジェンスを実施しているという。NSO のスタッフは輸出先の国を調査し、人権記録を調べ、イスラエルとの関係を精査する。スタッフは特定の機関の汚職、安全性、財政、乱用に関する実績を評価するとともに、販売先がどれだけツールを必要としているかも考慮している。

時には、ネガティブ情報がポジティブ情報を上回ることもある。例えば、モロッコは人権問題が悪化しているが、安全保障の面でイスラエルや西

側諸国と協力してきた長い歴史があり、実際にテロの問題も抱えているため、販売が認められた。対照的に、NSO は中国、ロシア、イラン、キューバ、北朝鮮、カタール、トルコなどを含む 21 カ国を顧客として認めていない。

最終的に、販売前に NSO のガバナンス・リスク・コンプライアンス委員会の承認が必要だ。経営陣と株主で構成されるこの委員会は、販売の拒否や条件追加、技術的な制約などを決定する権限を持ち、決定はケース・バイ・ケースで下されるという。

悪用の防止もしている

いったん販売が合意されれば、技術的なガードレールによってある種の悪用を防止できると NSO は主張している。例えば、ペガサスは米国人の電話番号を対象とした感染は許可されておらず、感染した携帯電話は物理的に米国に存在することさえ不可能だという。もし米国の国境内でペガサスに感染した携帯電話があれば、ペガサス・ソフトウェアは自己破壊することになっているという。

加えて、NSO はイスラエルの電話番号も保護されていると話すが、誰がなぜ保護されているのかは不明のままだ。

悪用の報告が入ると、NSO の従業員最大 10 人で構成される臨時チームが召集されて調査する。疑惑について顧客を聴取し、ペガサスのデータログを求める。このログには、チャットやメールなどスパイウェアが抽出したコンテンツは含まれていない（NSO は特定の情報は見ていないと主張）が、スパイウェアを感染させようとしたすべての電話と、その時点での位置情報などのメタデータは含まれている。

本誌が入手した最近の契約書によると、顧客は「犯罪やテロリズムの検出、防止、調査のみにこのシステムを利用し、人権侵害には利用しない」ようにしなければならず、悪用の可能性について顧客は NSO に伝えなければならないとされている。NSO は、過去にペガサスの悪用などの違反によって契約を 3 件打ち切ったことがあると述べ

ているが、どの国や機関が関与していたのか、あるいは被害者が誰なのかは明らかにしていない。

「我々の認識が甘いわけではない」

問題は透明性の欠如だけではなく、ガードレールの限界だ。イスラエル政府は、輸出法違反でNSOのライセンスを取り消せるが、規制当局は潜在的な顧客による悪用を進んで調べることはなく、NSOの悪用に関する調査にも関与しない。

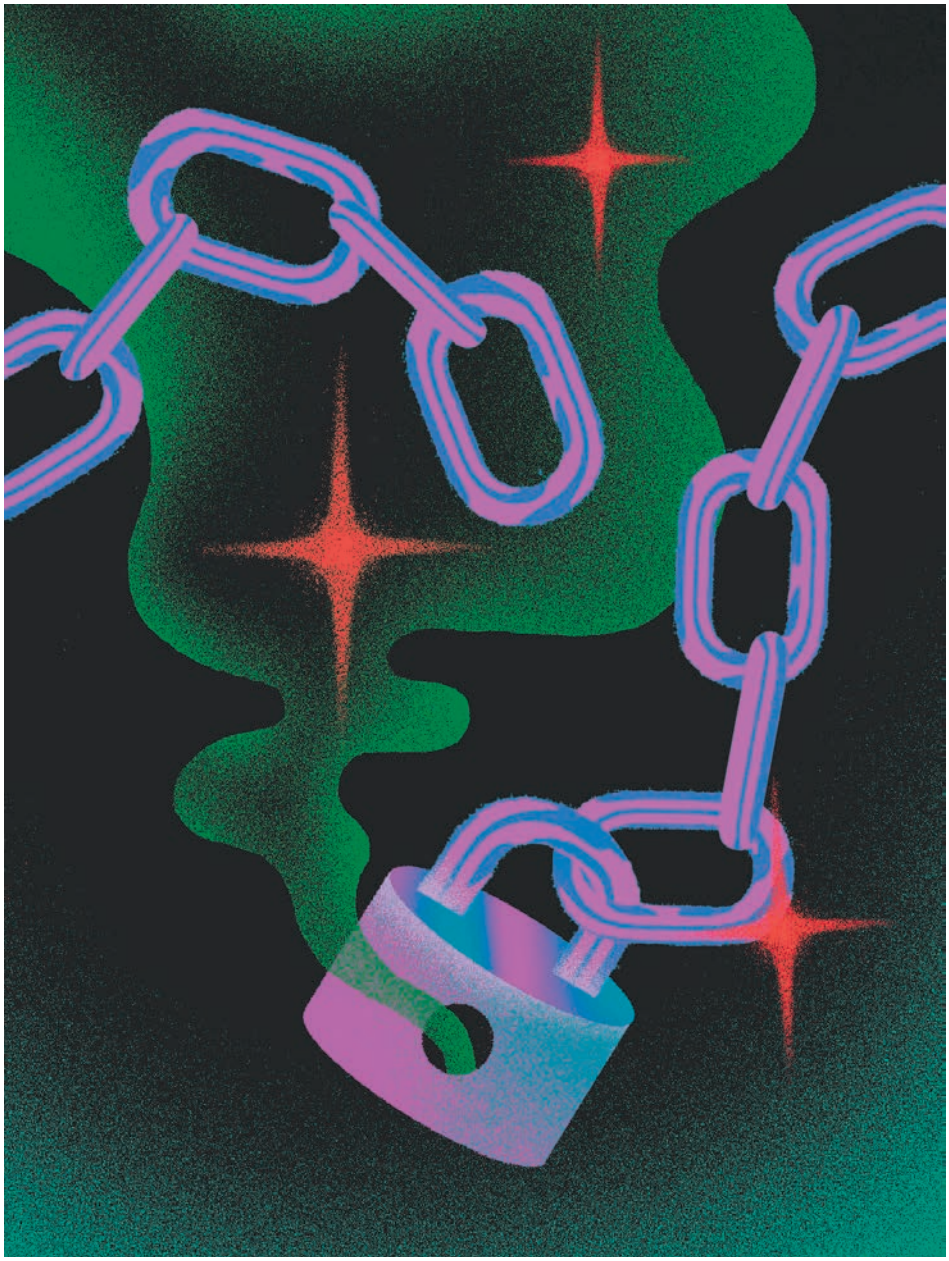
他の多くの措置も、単に対症療法をしているだけだ。多くの10億ドル規模のテック企業とは異なり、NSOには社内に常設の悪用対策チームはなく、調査のほとんどは国際人権団体アムネスティ・インターナショナル（Amnesty International）やトロント大学の研究機関シチズンラボ（Citizen Lab）など外部の情報源が違法行為を訴えた場合にだけ急ごしらえで実施される。NSOのスタッフは調査の中で機関や顧客から聴取はするが、被害者とされる人と話すことはない。また、NSOは証拠として提供された技術報告書に異議を唱えることが多いが、国家機密と企業機密の両方が原因で、より多くの情報を共有できないとも主張している。

どの悪用調査にも不可欠なペガサスのログも、多くの問題を引き起こす原因となる。NSOの顧客はスパイ機関で働くハッカーたちだ。その彼らにとって、ログの改ざんが難しいわけがない。NSOは改ざんは不可能だと主張したが、詳細については明らかにしなかった。

もし、ログに問題がないとすれば、NSOは顧客と一緒にターゲットの選び方が合法的か、真の犯罪が実施されたか、正式な法の手続きの下での監視か、独裁政権が反対勢力をスパイしたかどうかを判断することになる。

「もどかしい」。サンレイ部長は憤慨した様子で、秘密保持のせいでまるで手を後ろに縛られた状態で活動しなければならないと話した。

「我々の認識が甘いわけではありません。悪用はあったし、これからもあるでしょう。我々は多くの政府に販売しています。米国政府にさえもです。完璧な政府は1つもありません。悪用される



ARIEL DAVIS

可能性はあり、対処が必要です」。

しかし、サンレイ部長も NSO の標準的な回答、ワッツアップの訴訟における NSO の防御を支える主張を繰り返す。つまり、NSO は製造業者ではあるがスパイウェアの運営者ではなく、NSO は製造したが ハッキングをしたのは彼ら、つまり主権国家だ、という主張だ。

多くの批評家にとって、それは十分な説明では

ない。オランダ出身の政治家で、欧州議会の元議員であるマリーチェ・シャーケは、「自社製品の独立した監視機関になれると信じる企業に、私は納得しません」と話す。「NSO 独自のメカニズムを持っている一方で、人権擁護活動家やジャーナリストに対して使用されていることを知っていながら、商用スパイウェアを誰に販売しても問題ないという、その考え方そのものが、何よりこの会社の責任感の欠如を示していると思います」。

ではなぜ今ごろになって、内部の透明性を高めようと動いているのか？ それは人権団体から技術的な報告書が殺到し、ワッツアップの訴訟や政府による監視の強化によって NSO の現状が脅かされているからだ。また、業界がどのように規制されるかについて新しい議論が起こる場合、強力な発言力を持つことが必要だからだ。

暴かれる秘密

合法的なハッキングやサイバースパイ活動は、この 10 年間でビジネスとして急成長し、衰退する気配はない。NSO の前オーナーたちは 2014 年に 1 億 3000 万ドルで同社を買収したが、これは NSO が 2019 年に売却されたときの評価額の 7 分の 1 以下の金額だ。この業界自体も、通信技術の普及や深刻化する不安定な世界情勢によって利益を得て拡大している。アムネスティのダナ・イングルトン副理事長は「犯罪やテロリズムと戦うために、どの国にもハッキングや監視テクノロジーを購入する権利があります」と話す。「国家は正当かつ合法的に、そうしたツールを使用できます。しかし、それには悪用を防止し、悪用が起きた場合に説明責任を果たす仕組みを提供する規制を、制度として設ける必要があります」。ハッキング産業をより白日の下にさらすことで、規制の改善と説明責任の強化が可能になるとイングルトン副理事長は主張する。

2020 年初め、イスラエルの裁判所で、アムネスティはペガサスの乱用に関して国防省に NSO のライセンスを取り消すべきだと主張した。しかし、裁判が始まると、アムネスティの関係者と 29 人の原告は、退廷を命じられた。国防省の要

eムックは、MITテクノロジーレビュー
有料会員限定サービスです。
有料会員はすべてのページ（残り68ページ）を
ダウンロードできます。

ご購読はこちら
https://www.technologyreview.jp/insider/pricing/

No part of this issue may be produced by any mechanical, photographic or electronic process, or in the form of a phonographic recording, nor may it be stored in a retrieval system, transmitted or otherwise copied for public or private use without written permission of KADOKAWA ASCII Research Laboratories, Inc.

本書のいかなる部分も、法令または利用規約に定めのある場合あるいは株式会社　角川アスキー総合研究所　の書面による許可がある場合を除いて、電子的、光学的、機械的処理によって、あるいは口述記録の形態によっても、製品にしたり、公衆向けか個人用かに関わらず送信したり複製したりすることはできません。