many believe was the intended target. "This virus could only have been developed by a team of sophisticated security professionals with time and money at their disposal," explained Mikko Hypponen, chief research officer for F-Secure, a Finnish antivirus company. "We have known about it for several months and still haven't managed to decode it fully." This means, he said, that "we now have proof that states are investing serious resources into the development of next-generation viruses. It is without question the most significant virus we have seen in a decade."

There has been a ferocious debate as to the origins of Stuxnet. Most speculation lays responsibility at Israel's door; some respected researchers have implicated the United States, and others China. But it is still impossible to identify with any certainty the origin of a virus, especially if it is let loose into the world by a competent spy agency, as likely was the case with Stuxnet.

In fact, this virus has acted as the starting gun for an arms race in cyberspace. Not only do all major powers feel compelled to develop threatening malware; many smaller countries, which could not possibly compete in a conventional arms race, are working feverishly to develop cyberweaponry. It may sound as though it's an extension of a Bruce Willis movie, but Stuxnet provides proof that cannot be refuted: the global cybergame has begun. ■

Rise of the Digital Natives

How the battle for the Internet politicized prankster cybercollectives like Anonymous.

by LAURIE PENNY

The kid in the dock could be auditioning for a starring role in the global psychodrama *The Little Guy Versus the State*. Pale, thin and dwarfed by two enormous security guards in London's Westminster Magistrates' Court, Jake Davis speaks in a whisper, and only to confirm his name. He is 18, from the remote Scottish archipelago of Shetland, and he is accused of being a key agent in an international cyberactivist collective called LulzSec, which has attacked the web operations of entities ranging from the CIA to the Murdoch media empire. Davis is being charged with five computer-related offenses, including an attack on a major British police website and three counts of conspiracy. He seems to shrink inside his checked shirt, clutching a paperback titled *Free Radicals: The Secret Anarchy of Science*.

EDWIN VAZQUEZ

Hackers come in many forms, from criminals stealing credit card details to shadowy government organizations attacking enemy nuclear facilities; but today the most prominent and controversial are cyberactivists—or "hacktivists," as Davis is alleged to be. Loosely affiliated and rapidly expanding, these groups have thousands of members all over the world and names like AntiSec (which stands for "anti-security") and, most famously, Anonymous. These groups represent a new front in what has been labeled the "global information war": the growing battle over who controls information in cyberspace.

Operating anonymously, mainly via Internet relay chat (IRC) channels, hacktivist groups crash websites, hack servers and steal passwords. Their signature move is the DDoS (Distributed Denial of Service) attack, which involves coordinating thousands of computers to send traffic to a website until it overloads, crashes and shuts down—the digital equivalent of a sit-in, except that coordinating a sit-in does not usually earn you ten years' jail time, which is what Davis faces if found guilty.

Hackers have traditionally been chat room pranksters; one of the accusations against Davis is his alleged role in hacking the *Sun*'s homepage, redirecting readers to a fake news story telling the world Rupert Murdoch was dead. There are snickers from the press bench as the prosecution reads the charge, and Davis finds it impossible to stop the littlest of grins from creeping across his face. For cyberactivists, it has always been about poking fun: an anarchic collision of satire and direct action that makes a mockery of the powerful and self-satisfied. They do it "for the lulz," in cyberspeak.

Over the past year the work of these groups has become increasingly linked with a more serious mission, one that combats censorship on the Internet, whether by companies or governments. Anonymous in particular has become a powerful collective. At the Occupy Wall Street protests in New York, which Anonymous helped promote, young people wandered through the crowd in plastic Guy Fawkes masks—a symbol of collective, innominate popular resistance from the film and graphic novel *V for Vendetta*, which has been adopted by the group. In support of the protests, which target corporate greed and economic inequality, Anonymous posted a video online threatening to erase the New York Stock Exchange "from the Internet." Elsewhere in Liberty Plaza, young tech activists gave lectures on digital freedom and uploaded open-source software free of charge for anyone who'd brought along a laptop. Technology plays an essential role in the new networked people's movements that are springing up all over Europe, America and the Middle East—and those movements have brought cyberactivism into its own. The generation that was supposed to be made listless and apathetic by technology—

Laurie Penny, a writer, journalist and activist from London, writes regularly for The New Statesman *and the* Independent. *She is the author of* Penny Red: Notes From the New Age of Dissent.

the kids who were supposedly staring vacantly into virtual worlds in lonely bedrooms—are instead using technology to re-engage with current events in an era when the very principles of power are being rewritten on terms not wholly in the control of nation-states.

"There's not a whole lot of historical precedent" for cyberactivism on this scale, says Gabriella Coleman, who lectures on technology and anthropology at New York University. "It's hard to say what's going to happen, except that states are going to clamp down quickly."

Most security experts agree that sophisticated cyberattacks by nation-states, like the Stuxnet attack on an Iranian nuclear facility last year, are a far greater threat to global security than autonomous hacking collectives knocking out company websites. The former is the digital equivalent of state espionage; the latter, the equivalent of a road blockade or banner drop. Nonetheless, the FBI and other law enforcement bodies are concentrating a great deal of effort on these cyberprotesters. The United States has spent the past year recruiting hundreds of "white hat" hackers to fight cyberactivism and e-crime and has launched a global manhunt for members of Anonymous, LulzSec and other groups. It's also leaning on other countries to take similar measures: under US pressure, Japan is considering requiring companies to share information about hackers with the government.

As the attacks have become more political—with more law enforcement agencies and major companies becoming targets of protest hacks—so has the backlash. Since this past summer, many suspected members of Anonymous, LulzSec and other groups, some of them as young as 16, have been arrested in Europe and North America in a series of sting operations. Yet the attacks have continued, targeting, among others, more than seventy police websites across the United States and the Syrian ministry of defense website, where the group posted a message of solidarity with the Syrian people. The iron-fisted response to relatively benign cyberactivism seems only to breed more of the same while diverting resources that could be used to pursue the type of cybercrime that actually poses a public threat.

Like so much on the Internet, in a way, contemporary hacktivism started with porn. Anonymous, for example, originated in the chat site 4chan, whose message boards are scurrilous back-channels full of filthy in-jokes.

Early DDoS attacks, starting in February 2010, targeted Australian authorities who tried to censor the distribution of cyberporn—a project code-named Operation Titstorm—as well as a proxy company that attempted to bring down The Pirate Bay, a file-sharing site for downloading music and videos. At stake was not so much nude photos or free MP3s but the very principle of free information exchange. In this sense, the trajectory of hacktivism from defending free file sharing to defending freedom itself may have been inevitable. "It started off with exposing titty videos to their friends," explains one member of the militant "tech dissent" collective DSG (Deterritorial Support Group), who identifies as Zardoz. "It ended with bringing down [an] autocratic regime."

He (or she) is referring to the Egyptian revolution, a key moment of politicization for cyberactivists, who stepped in to help the rebels with communications after Hosni Mubarak shut down the Internet. As the Arab Spring and subsequent global upheaval of the summer demonstrated, the fight for freedom of speech and action online has become enmeshed with the offline struggle for freedom of movement and thought. The "politicization of 4chan," as this trajectory is partially known among hacktivists, can be traced to WikiLeaks. After the whistleblowing website released thousands of classified documents and diplomatic cables last fall, MasterCard and PayPal announced they would suspend payments to WikiLeaks, prompting members of Anonymous to shut down the companies' websites. Titled Operation Payback, the project changed the rules of engagement for those cyberactivists who had previously seen their anticensorship activities as separate from geopolitics. In this sense, WikiLeaks's great triumph has been to make the world think again about whether governments should have the right to withhold information from citizens and obstruct the free exchange of ideas online.

For young people around the world who grew up with the Internet—"digital natives"—the question is both profound and profoundly uncomplicated. Defending the freedom to share information online is more important than individual politics or morality. "That's why Anonymous intervened in Wikileaks," explains Zardoz. "That's why they intervened in Tunisia. And that's why they intervened in Egypt." In Operation Egypt and Operation Tunisia, Anonymous and other groups coordinated to restore citizens' access to websites blocked by the government. The efforts extended beyond the Internet, with faxes used to communicate vital information as a means of last resort. (In classic "lulzy" style, cyberactivists also caused havoc by ordering enormous quantities of pizza delivered to Egyptian and Tunisian embassies.)

After Egypt, it became clear that the fight against censorship and the fight against state oppression were moving closer together. "This is not a minor struggle between state nerds and rogue geeks," wrote members of the DSG collective in June, in an influential blog post titled "Twenty reasons why it's kicking off in cyberspace." "This is the battlefield of the 21st Century, with the terms and conditions of war being configured before our very eyes."

On this point, hacktivists and security experts agree. "LulzSec and Anonymous are exposing the huge number of vulnerabilities that are out there waiting to be exploited by someone who has the skills and the motivation," says Chris Wysopal, co-founder of Veracode, a security company based in Massachusetts. "Data is so leaky," says NYU's Coleman, "and if all you need to crack a government facility is a USB stick, can we really stop that happening?"

That's precisely the question that has state powers running scared. In these unsteady times, one of the few things we can know with any certainty is that the future is digital; the Internet—and the possibilities for collective engagement and disruption it offers—is not going away. It would take a massive worldwide program of censorship and surveillance both on- and offline to crack down on this, and that's just what "tech dissidents" are hoping to prevent.

The link between dissent by technology and dissent in the streets is growing stronger. The fact that ordinary citizens can get and share information instantaneously not only provides them with the tools to resist authority and evade arrest; it also delegitimizes that authority on practical and philosophical levels. Controlling information, after all, is one of the most important ways a state wields its power. Over nineteen months that have seen the nature and structure of power called into question around the globe, the nature and structure of technological dissent have grown and matured in kind. To police, the press and the powerful, this evolving link between technology and dissent is cause for alarm: nobody knows what cyberactivists might be capable of next.

Ultimately, one person's cyberterrorist is another person's digital freedom fighter, and for many, that's precisely what hacktivists are. In Liberty Plaza, the nerve center of the Occupy Wall Street protest is a makeshift media tent full of serious young people fussing over laptops in tangles of cables. Not all cyberactivists are young—stereotyping hacktivists as adolescent recluses is an easy way to dismiss their ideas—but there's one thing that teenagers and technologies can do far faster than grown-ups and governments, and that's adapt. ■

The GOP's Deregulation Obsession

Republican pals of big business have launched "the Contract With America on steroids."

by ROBERT WEISSMAN

It's hard to imagine a worse time for big business to conduct a full-blown attack on regulatory protections. The country continues to suffer from a deep recession caused in large part by financial deregulation and underenforcement of existing rules. A string of corporate disasters—the BP oil gusher, the Massey coal mine explosion, unintended acceleration in Toyota cars, leaded toys, killer cantaloupes—all tied directly to inadequate regulatory protections, are fresh in the public mind.

EDWIN VAZQUEZ

For the US Chamber of Commerce, however, the facts shouldn't get in the way of a stupendous power grab. The Chamber and its allies on Capitol Hill have launched an unprecedented antiregulation campaign, with the goal of blocking new safeguards against corporate wrongdoing and rolling back environmental, health, financial and other regulatory protections.

"The current situation might be characterized as the Contract With America on steroids," says Gary Bass, former executive director of OMB Watch, a DC-based advocacy group, noting political factors that make this period more dangerous than the mid-1990s. "First, these antiregulatory advocates are using high unemployment as a wedge, claiming that regulations are job killers. Second, antiregulatory forces have developed a powerful message machine." That message, which is being funded to the tune of millions of dollars, is visible across the street from the White House, where the facade of the Chamber of Commerce is covered with a giant banner that reads: JOBS. This is the overriding public rationale for its agenda: the Chamber and its allies have created an echo chamber to describe public protections as "job-killing," imposing burdens on the "job creators" (corporations) and preventing them from undertaking new investments. The Chamber has even created an online board game, Thiswaytojobs.com.

In reality, it was insufficient controls on Wall Street that facilitated the financial crash and the Great Recession, which threw 8 million people out of work. Even when they impose modest short-term costs on businesses, health, safety and environmental protections also commonly create jobs by spurring innovation to address new standards. But opponents of public protections discard such evidence, relying instead on deceptive studies written by those committed to bolstering their deregulation crusade. One preposterous report, issued by consultants to the Small Business Administration, twists a dubious index from the World Bank to conclude that the annual US regulatory burden is $1.75 trillion. This cost estimate largely depends on opinion polls of business leaders while ignoring the benefits of regulations altogether. Even the Bush administration found regulatory benefits to be at least twice as great as costs.

Yet intellectually hollow arguments have gained traction. Darrell Issa, chair of the House Oversight and Government Reform Committee, set the stage for the GOP obsession with deregulation in December, when he wrote to 150 trade associations and business-linked think tanks requesting a wish list of regulatory safeguards they would like to see blocked or repealed. Trade associations from the American Coke and Coal Chemicals Institute to the American Meat Institute answered the call. House Republicans have introduced at least twenty-eight antiregulatory bills, according to a tally by the Center for Progressive Reform.

Blocking regulatory protections has emerged as the centerpiece of the Republicans' purported jobs plan. In August Eric Cantor, the House majority leader, laid out their fall legislative agenda, focused on blocking "job-destroying regulation." Cantor has House Republicans pushing ten bills to enable cor-

Robert Weissman is president of Public Citizen, which co-chairs the Coalition for Sensible Safeguards.