When the Internet was created, decades ago, one thing was inevitable: the war today over how (or whether) to control it, and who should have that power. Battle lines have been drawn between repressive regimes and Western democracies, corporations and customers, hackers and law enforcement. Looking toward a year-end negotiation in Dubai, where 193 nations will gather to revise a U.N. treaty concerning the Internet, Michael Joseph Gross lays out the stakes in a conflict that could split the virtual world as we know it.

I. Time Bomb

In 1979 the Dubai World Trade Centre dominated the skyline of Dubai City, on the horn of the Arabian Peninsula. Today, the World Trade Centre looks quaint, like an old egg carton stuck into the ground amid a phantasma-goric forest of skyscrapers. But come December the World Trade Centre will once more be the most important place in Dubai City—and, for a couple of weeks, one of the more important places in the world. Diplomats from 193 countries will converge there to renegotiate a United Nations treaty called the International Telecommunications Regulations. The sprawling document, which governs telephone, television, and radio networks, may be extended to cover the Internet, raising questions about who should control it, and how. Arrayed on one side will be representatives from the United States and other major Western powers, advocating what many call "Internet freedom," a plastic concept that has been defined by Secretary of State Hillary Clinton as the right to use the Internet to "express one's views," to "peacefully assemble," and to "seek or share" information. The U.S. and most of its allies basically want to keep Internet governance the way it is: run by a small group of technical nonprofit and volunteer organizations, most of them based in the United States.

On the other side will be representatives from countries where governments want to place restrictions on how people use the Internet. These include Russia, China, Brazil, India, Iran, and a host of others. All of them have implemented or experimented with more intrusive monitoring of online activities than the U.S. is publicly known to practice. A number of countries have openly called for the creation of a "new global body" to oversee online policy. At the very least, they'd like to give the United Nations a great deal more control over the Internet.

Mediating these forces in Dubai will be a man named Hamadoun Touré. Charming and wily, he is a satellite engineer who was born in Mali, educated in the Soviet Union, and now lives in Geneva. He serves as secretary-general of the U.N.'s International Telecommunication Union (I.T.U.).

Touré abjures pallid diplomatic doublespeak, instead opting for full-on self-contradiction that nonetheless leaves little doubt where his sympathies lie. In one breath Touré says, “The people who are trying to say that I.T.U. has an intention of taking over the management of the Internet simply do not know how the I.T.U. is functioning.” In the next, noting that Internet users in America represent only a tenth of the total, he says, “When an invention becomes used by billions across the world, it no longer remains the sole property of one nation, however powerful that nation might be. There should be a mechanism where many countries have an opportunity to have a say. I think that’s democratic. Do you think that’s democratic?”

There is a war under way for control of the Internet, and every day brings word of new clashes on a shifting and widening battlefront. Governments, corporations, criminals, anarchists—they all have their own war aims.

In February, the Swedish Supreme Court refused to hear appeals from three founders of the Pirate Bay, the world’s largest illegal file-sharing Web site, who had been sentenced to prison for copyright infringement. The same day, one of those men issued an online call to arms, urging users to abandon the entertainment industry: “Stop seeing their movies. Stop listening to their music.... Remix, reuse, use, abuse.” Shortly after that, Google was discovered to have been secretly bypassing privacy settings on Apple iPhones and computers that use the Safari browser; the company was monitoring Web activity by people who believed they’d blocked such tracking. Around the same time, the European Union proposed that companies such as Google must obtain explicit consent from individuals for data collection; but these regulations would not take effect for years, by which point digital dossiers on almost every Internet user will have been bought and sold by marketers many times over. Meanwhile, the F.B.I. has been distributing “See something, say something” flyers to Internet-café owners in the U.S., warning that the use of certain basic cyber-security measures could be considered grounds for suspicion of possible terrorist activity. In response to the F.B.I.’s growing preoccupation with virtual insurgents, guerrilla hackers operating under the name Anonymous posted online an audio recording of F.B.I. and Scotland Yard officials discussing how to handle Anonymous attacks. Then Interpol, together with American and European authorities, busted 31 suspected Anonymous hackers—including the one who covertly recorded that conference call—and an F.B.I. official declared victory over LulzSec, one of the most prominent Anonymous splinters, with the boast that “we’re chopping off the head” of that faction.

The War for the Internet was inevitable—a time bomb built into its creation. The war grows out of tensions that came to a head as the Internet grew to serve populations far beyond those for which it was designed. Originally built to supplement the analog interactions among American soldiers and scientists who knew one another off--line, the Internet was established on a bedrock of trust: trust that people were who they said they were, and trust that information would be handled according to existing social and legal norms. That foundation of trust crumbled as the Internet expanded. The system is now approaching a state of crisis on four main fronts.

The first is sovereignty: by definition, a boundary-less system flouts geography and challenges the power of nation-states. The second is piracy and intellectual property: information wants to be free, as the hoary saying goes, but rights-holders want to be paid and protected. The third is privacy: online anonymity allows for creativity and political dissent, but it also gives cover to disruptive and criminal behavior—and much of what Internet users believe they do anonymously online can be tracked and tied to people's real-world identities. The fourth is security: free access to an open Internet makes users vulnerable to various kinds of hacking, including corporate and government espionage, personal surveillance, the hijacking of Web traffic, and remote manipulation of computer-controlled military and industrial processes.

There is no agreement about how any of these problems should be solved. There isn't even agreement on how to define the basic terms of debate. "Internet freedom," for instance, is the avowed objective not only of the U.S. secretary of state but also of Wiki-Leaks, which published hundreds of thousands of classified State Department diplomatic cables.

One way to think about the War for the Internet is to cast it as a polar conflict: Order versus Disorder, Control versus Chaos. The forces of Order want to superimpose existing, pre-digital power structures and their associated notions of privacy, intellectual property, security, and sovereignty onto the Internet. The forces of Disorder want to abandon those rickety old structures and let the will of the crowd create a new global culture, maybe even new kinds of virtual "countries." At their most extreme, the forces of Disorder want an Internet with no rules at all.

A conflict with two sides is a picture we're used to—and although in this case it's simplistic, it's a way to get a handle on what the stakes are. But the story of the War for the Internet, as it's usually told, leaves out the characters who have the best chance to resolve the conflict in a reasonable way. Think of these people as the forces of Organized Chaos. They are more farsighted than the forces of Order and Disorder. They tend to know more about the Internet as both a technical and social artifact. And they are pragmatists. They are like a Resistance group that hopes to influence the battle and to shape a fitful peace. The Resistance includes people such as Vint Cerf, who helped design the Internet in the first place; Jeff Moss, a hacker of immense powers who has been trying to get Order and Disorder to talk to each other; Joshua Corman, a cyber-security analyst who spends his off-hours keeping tabs on the activities of hackers operating under the name of Anonymous; and Dan Kaminsky, one of the world's top experts on the Internet's central feature, the Domain Name System.

Although they may feel a certain kinship with one another, they are not an organized group. Their main point of agreement is that the Internet has changed the world forever, in ways we are only beginning to understand. They know that Order is impossible and that Disorder is unacceptable. They understand that the world is a messy place whose social arrangements come and go. But they are united in the conviction that what must be preserved and promoted at all costs is what the forces of Order and Disorder, in their very different ways, are both intent on undermining: the integrity of the Internet itself as a reliable, independent, and open structure.

II. Free-for-All

Vint Cerf knew from the start that there was a problem—he just couldn’t fix it. The year was 1975, and Cerf was on a team of computer scientists at Stanford University under contract to finish a new communications network for the U.S. military. The goal was full cryptographic capability—a system that allowed all messages to be authenticated from both sides—on a network that could be used anywhere in the world. Two things prevented the scientists from making this network as secure as they would have liked. One obstacle was institutional: “The only technology that would have allowed for such security was still classified at the time,” Cerf recalls. The other obstacle was simple momentum. Before the developers could implement truly secure encryption, Cerf explains, “the system kind of got loose,” meaning that problems would have to be fixed on the fly.

Cerf is frequently referred to as “the father of the Internet.” His most celebrated achievement, for which he shares credit with the engineer and computer scientist Robert Kahn, was creating the TCP/IP protocol, the system that allows computers and networks all over the world to talk to one another. He was an early chairman of the Internet Corporation for Assigned Names and Numbers, or icann, which maintains the Domain Name System, the virtual address book that shows your computer where to go when you type the name of a Web site into your browser. He now works as Internet Evangelist—that’s his actual title—for Google.

Most of the Internet’s problems, Cerf believes, stem from the issue of state sovereignty. The Internet was designed to ignore national boundaries. It was designed this way, Cerf says, because “it was intended to deal with a military problem”: how could soldiers exchange messages without letting their enemies know where they were? Cerf and others solved that problem by building a decentralized network that routed mes-sages from place to place using addresses that had nothing to do with physical locations.

This was something new. International telephone transmissions were marked with country codes that named their origins and end points and had to pass through central switches in the countries at both ends. Radio transmissions, similarly, had to hop from the fixed points of towers. On the Internet, by contrast, traffic skittered from place to place on a network whose shape could be in constant flux. The Internet had no center at all.

With one exception. The sole centralized feature of the Internet was the Domain Name System. The United States created that system, which lives on root servers, and Americans maintained it even as the Internet started spreading. The first thing your computer does when you type a Web site or e-mail address into your browser is to ask a local D.N.S. server for the numerical IP address of that destination. Because the D.N.S. servers are the first stop, the D.N.S. is not just the Internet's address book. It's also the corner post office. Whoever runs the D.N.S. system can potentially control whether your browser requests get to the proper place and thus control where you can and can't go online.

By the mid-1990s, the Internet was teeming with life, some of it dangerous or unpleasant. Certain aspects of the unpleasantness were inadvertently self-created. Since World War II, the U.S. government had classified cryptography as a munition, subject to stringent export controls. In the Internet's first decades, those restrictions made it difficult to do business securely online. No one liked the prospect of making financial transactions on the Web without strong encryption, and international transactions were impossible unless parties in both countries used the same encryption techniques. So in 1997, President Bill Clinton relaxed export controls on encryption. This had the unintended effect of giving criminals new ways to steal intellectual property: now they could easily encrypt what they took and send it out of the country, to Russia, China, or elsewhere. Those criminals pioneered the systematic exfiltration of intellectual property that plagues American business today.

Loosening export controls also had the effect—and this was very much intended—of commercializing the Internet. In fact, the Clinton administration was creating something close to an online free-for-all with its determined efforts to make the Net an engine for business. But even after the encryption export controls were relaxed, businesses outside the U.S. remained wary of the Internet, thinking of it as a de facto American protectorate. Its one centralized feature, the Domain Name System, remained under U.S.-government control.

Clinton had seen that problem coming, and had already set out to turn the D.N.S. over to the private sector. The result was icann, a nonprofit body whose advisory committees include representatives of more than 100 countries and scores of corporations. Technically,
icann

remains under the Commerce Department's authority, but other governments have a meaningful say in the group's decisions. For instance, Xiaodong Lee, one of China's Internet czars, is icann 's vice president for Asia. The creation of icann signaled that the Internet would be something akin to global patrimony, not an online version of American soil.

This shift helped set the Internet free. But the more the global economy came to depend on the Internet, the harder it was for governments to tame or limit it. This, too, was intentional. To ensure a surge of e-commerce, the administration systematically pushed aside or revised whatever might stand in the way, including taxes, tariffs, regulations, and intellectual-property standards. Grabbing with both hands for the Internet economy meant letting go of old ideals of governance.

Whole new problems eventually arose as markets and communications moved online, and as all these online exchanges were preserved digitally and became searchable. Who owned all this data? Who should have access to it? Corporations such as Microsoft, Google, and Facebook began butting heads with the government. They also began butting heads with their own customers.

Corporate ambitions are a huge issue, but "the real War for the Net," Cerf believes, "is governments who want to control it, and that includes our own government. If you think about protecting the population and observing our conventional freedoms, the two are real-ly very much in tension." Cerf cites the debate over the U.S.A. Patriot Act, enacted in 2001, which greatly expanded the U.S. government's domestic-surveillance authority. He also cites efforts by Middle Eastern governments to control online communications, particularly as the Arab Spring began to unfold, in 2011. And then there's the vast example of China, whose Great Firewall puts severe limits on what Chinese users can view online.

On the Internet, what constitutes a "government" anyway? When Google announced in 2010 that it had fallen victim to Chinese hackers, it chose to publicize the fact that the Gmail accounts of Chinese political dissidents had been compromised. Congressional staffers asked company officials at the time about rumors that Google's data losses were in fact far more extensive. They recall tense conversations with Google executives, who in effect asserted executive privilege. One Hill aide recalls, "Clearly these people are used to having their way with everybody, which pissed us off. Because they are not a state within a state, even though they practically claim sovereignty.”

III. The Dark Tangent

Dead Addict remembers his hand trembling as he dialed the number. What, he wondered, was the point of even making the call? He stopped, reminding himself: the Dark Tangent was counting on him.

In 1992, a very young man named Jeff Moss, whose hacker name is the Dark Tangent, wanted to meet some friends he’d made online. So he organized a summer gathering in Las Vegas, which he planned to call “Def Con,” short for “defense condition” (defcon), the military’s term for its worldwide alert posture. Changes in defcon—a numbered scale from 1 (war) to 5 (peace)—had cued the turning points in *WarGames,* a movie that made the young Jeff Moss aspire to become a hacker in the first place. Moss had high hopes. For one thing, he wanted Def Con to be a great party. He also wanted to start “building a system of checks and balances” between hackers and law enforcement, two cultures that were becoming bitter adversaries. So when his friend Eli, who goes by the name Dead Addict, volunteered to help Moss plan the gathering, Eli got the job of calling one of the hackers’ arch-nemeses, an assistant attorney general in Arizona named Gail Thackeray, and inviting her to come.

Two years earlier, Thackeray had helped the U.S. Secret Service run Operation Sun Devil, one of the first crackdowns on illegal computer hacking. A lot of hackers hated Thackeray, and Dead Addict was not surprised when she responded to his invitation with the words “No. I wouldn’t go to a convention of car thieves, either.”

Hackers are nothing if not persistent, and Thackeray was eventually persuaded to spend a few days in the kiln that is Vegas in July. In a fire-engine-red blazer, she listened impassively while hackers as young as 14 described how to crack into every imaginable “secure” computer system. The hackers, for their part, eagerly picked Thackeray’s brain, to learn the legal implications of their recent and planned adventures. As Moss remembers, Thackeray frequently interrupted their questions to insert the word “hypothetically” in order to make herself feel a little better about being there.

Every summer, Moss uses Def Con to promote conversation between the Internet’s forces of

Order and Disorder. He has become the go-between who translates his subculture's concerns to the culture at large, and vice versa. Each year, more and more law-enforcement, military, and intelligence personnel go to Def Con. On the cusp of early middle age, Moss remains boyish-looking. He wears rimless oval glasses and favors long, silk-lined Shanghai Tang coats. Moss has become a powerful man. He sits on the U.S. government's Homeland Security Advisory Committee, and he serves as the chief security officer for icann.

Where Vint Cerf argues that sovereignty lies at the heart of the War for the Internet, Moss—who as a hacker cut his teeth gaining access to systems and information that belonged to others—argues that the heart of the matter may be intellectual property. As Moss points out, before the Internet, when copyrighted information existed mostly in the form of physical objects, it was inconvenient to violate copyright law, for purely practical reasons. Then the Internet created a giant mashup of Alexandria, the Louvre, the *Times-Herald-News-World-Journal-Tribune,* and all of television, Hollywood, and the music industry. People started to feel existentially entitled to this wealth of information. As it became normal to post songs, video clips, essays, and stories—all copyrighted by other people—on Web sites, that sense of ownership increased. In many minds, it became not just a convenience but a right.

This transformation occurred during the same years the Internet became a place to do business. When social-media sites such as Twitter and Facebook merged those two functions—turning the common person's scrapbook into a cash cow for corporations—they sparked the Internet's next evolutionary adaptation. The consumer and the citizen now combined to form a complicated new species, most of whose members experienced the change as extremely empowering—even as they were also becoming extremely vulnerable. Individuals were using their free access to intellectual property to express themselves to one another—our Facebook "likes" equaled our actual "selves"—creating a phenomenon that is, for governments as well as corporations, the most tempting target imaginable. This trove of information is to an ordinary census database what a super-collider is to a slingshot.

Privacy advocates sounded alarms about the problem, but the 2009 Green Revolution protests in Iran were a major turning point. The ease with which the Iranian government spied on its own citizens—using techniques that anyone could deploy, with free and open-source software—showed the fundamental insecurity of all unencrypted data (which is almost all data) on the Internet. Iranian-government authorities were able to read citizens' e-mails, diagram their social networks, and keep watch on almost anything else they wanted to observe. The spectacle of that violation, Moss says, underscored for everyone that the character of the Internet had fundamentally changed. It had evolved from, as he puts it, a place "to put pictures of your cat" to a place where "your liberty's at stake."

Even so, the most influential Web sites, such as Google, Facebook, and Twitter, balked at adapting to the new reality they'd helped bring into existence. No communications on any of those sites were fully encrypted yet. Without mockery, Moss recites their arguments in a plain tone, strained only by mild weariness: "It's too expensive. We never designed it to be all encrypted. And, you know, the Net is not a private place anyway. It's not really our problem." His response, in the same tone, is that, since these corporations built their empires by encouraging everybody to share everything, they have a responsibility to provide security.

During that violent week in 2009, Iran also blocked its citizens' access to popular dissident Web sites. Government authorities hijacked the Internet's address book—using a technique called D.N.S. blocking—so that when people tried to organize via Facebook or Twitter, they got sent elsewhere. Today, as chief security officer for icann, Moss is implementing a set of technical changes that will eventually make it more difficult for anyone to engage in D.N.S. blocking—difficult, but not impossible. "I'm curious if it's fixable," Moss admits. "Everybody always calls it rebuilding the airplane in flight. We can't stop and reboot the Internet."

Technical constraints are complicated by politics. Not everyone approves of the changes Moss promotes. This winter, Congress considered two bills designed to stop online piracy. The Protect Intellectual Property Act (pipa) and the Stop Online Piracy Act (sopa) could have allowed the U.S. government to mandate D.N.S. blocking—the technique that Iran had used—to prevent Americans from seeing unauthorized postings of copyrighted material on social-media or search-engine sites. The bill might also have made those sites responsible for removing links to pirated material. The D.N.S.-blocking provision was dropped from the bills, whose other problematic features were still subject to revision. But a ferocious Web revolt, incited, in part, by Internet giants such as Reddit, Google, and Wikipedia, invoked the specter of censorship. The legislation was effectively killed.

According to Moss, people who want more government control of the Internet are saying, "Well, we'll just do this. We'll just do that." He says, "It's like, You just don't *do* that with the Internet. Don't have the legislator who doesn't understand how anything works make the decisions. The biggest fear is that you'll have governments around the world legislating technical standards. And then everything comes crashing down."

Besides, he goes on, "the more government tries to regulate, the more people will try to build an Internet that is uncensorable and unfilterable and unblockable"—with tools such as darknets, which are hidden networks that run on privately owned machines. On the other side, authoritarian governments want to build their own private Internets. The Iranian government has in fact launched a “halal” Internet, cut off from the rest of the world.

Even Moss, who participates in the highest-level discussions about global Internet policy, finds himself unable to keep up with all of the efforts to control the Internet that are happening right now. He says, “If you’re using an analogy of Internet wars, the battles are coming faster.” No sooner had sopa and pipa been scuttled than other legislation sprang up in their place in the U.S., Europe, and elsewhere. In January, after Poland signed an international copyright agreement that included provisions similar to those in sopa and pipa , a group of Polish legislators protested the vote by wearing Guy Fawkes masks—the visual emblem of Anonymous—inside the Polish parliamentary chamber.

One thing is clear. After this winter’s debates on piracy, it will be difficult for legislators to handle Internet policy the way they’ve handled so many other issues: by gentlemen’s agreements among interested parties. The intensity of protest will make that impossible. And the guerrillas have powerful weapons.

IV. The Summer of Lulz

The man known as Jericho said, “Raise your hand if you were never an asshole at some point in your career.” Not many hands went up. Last August, hundreds of people jammed into a ballroom at the Rio hotel in Las Vegas for a Def Con panel on hackers who operate under the name of Anonymous. The event was called “Whoever Fights Monsters”—a reference to Nietzsche: “Whoever fights monsters should see to it that in the process he himself does not become a monster.” Jericho’s line was a reference to Aaron Barr, the former C.E.O. of the cyber-security firm HBGary Federal. Several months earlier, Barr had plotted to discredit WikiLeaks by faking documents to make the group look unreliable. Then Barr investigated the Anonymous hackers who were supporting WikiLeaks, and boasted to the *Financial Times* that he had “collected information on their core leaders, including many of their real names.” In retaliation, Anonymous hackers annihilated Barr’s Web site, spilled HBGary’s archive of 71,000 e-mails onto the Web, raided Barr’s Twitter account, and remotely deleted everything from his iPad. Stephen Colbert summarized the event memorably: “Anonymous is a hornet’s nest, and Barr said, ‘I’m gonna stick my penis in this thing.’”

Jericho is known to the outside world as Brian Martin, a Denver cyber-security consultant. The objective of his discussion was to talk about—and to—Anonymous hackers. Some of them were in attendance. Jericho was hoping to nudge them toward using their power in constructive ways that minimize collateral damage.

He sat at a table onstage with Joshua Corman, whose day job is as director of security for a firm called Akamai. Corman, a compact, bearded man, tapped his fingers on the table, fiddling with his Starbucks coffee cup. A few months later, in Corman's dining room in the small New Hampshire town where he lives, we watched a video of the discussion. He recalled being almost paralyzed with nerves.

After the HBGary hack last February, the public image of Anonymous went split-screen. On the one hand, Anonymous operations supported the Arab Spring (and, later, Occupy Wall Street). On the other hand, a group of hackers identifying itself as a splinter of Anon, called LulzSec ("lulz" means "laughing out loud" at the victim of a prank; "sec" means security), launched a series of attacks that trashed all standards of privacy and security. The attacks, known as "the summer of lulz," were, on the whole, as pathologically anarchic as something the Joker might have done. LulzSec hacked Fox.com and leaked the contestant database for the show *X Factor,*
then posted a fake news story about Biggie Smalls and Tupac Shakur on the PBS Web site. When Arizona passed a Draconian immigration bill, LulzSec spilled online the personal contact information of hundreds of the state's policemen.

In many cases, Corman recalls, "there was no moral, or righteous, or freedom cause" behind the actions. "It was about having fun and breaking stuff." When he decided to speak publicly, Corman endorsed the goals of using the Web to effect political change and expose corruption, goals that Anonymous hackers sometimes cite. Even so, he could not stop worrying that by doing so he was putting himself and his family in harm's way.

Reporters generally refer to Anonymous as a "group" or, somewhat more accurately, as "a loose collective." Anonymous, Corman explains, is not real-ly a group, and it is a "collective" only insofar as there is some overlap among the individuals who perform the deeds attributed to Anonymous. "Anonymous is more like a brand or a franchise," Corman says—it's a term used by many individuals and groups with many ideologies for many kinds of actions. Hacking by Anonymous generally expresses a hunger for the complete transparency of governments and corporations. Anonymous hackers often oppose surveillance and promote self-government. Beyond these principles, there is little consensus. Corman compares Anonymous to a Rorschach blot, in which the forces of Order and Disorder alike see what they want to see.

With Jericho, Corman started tracking Anonymous last year. (This effort has nothing to do with his day job at Akamai.) On Corman's blog, the two offer what may be the most clear-eyed analysis of the Anonymous phenomenon available anywhere. Why, given the risks, does Corman pursue it? In some ways, the arc of his life seems to leave him little choice. He became the man of the household at age 14, after his parents' divorce. Like many children who prematurely take on adult responsibilities, he developed a fascination with power. For Corman, that fascination was nourished by the comic-book adventures of Spider-Man, a six-foot plastic statue of whom stands in the foyer of his house. He often quotes a famous Spider-Man line—"With great power comes great responsibility." Corman sometimes escaped from the burdens at home by diving into his computer. He compares his early experiences of programming, and of the Net, to a kind of sorcery.

Corman believes that the spread of "hacktivism," which first made mainstream headlines when Anonymous attacked the Church of Scientology in 2008, demonstrates that "those who can best wield this new magic are not nations. They're not politicians. The youngest citizens of the Net don't even recognize allegiance to a country or to a political party. Their allegiance is to a hive. In some ways this is very exciting. In other ways this is terrifying." The terrifying part, for Corman, is that the Web gives individuals immense power without instilling the "compassion, humility, wisdom, or restraint to wield that power responsibly."

Corman once jokingly referred to himself as "the guy with the Spider-Man statue who's gnashing his teeth in New Hampshire." Like everyone who understands the decentralized structure of the Internet, he is skeptical of government attempts to control it. He does harbor some hope, and it's partly a legacy of those comic books: "The most badass hackers I know get no satisfaction out of attacking. They prefer defending, because it's harder." He wonders if we're about to see the rise of another form of Internet vigilante, who will create tools to vanquish Anonymous attacks and deliver the miscreants by the scruff of the neck, as Superman would, to the government's doorstep. "Do the Avengers need to rise?" Corman asks. "When do they rise? They rise when the system doesn't sufficiently fight evil."

In the meantime, Anonymous has spawned a tiny cottage industry that keeps a very low profile: mercenary fighters hired by major corporations to protect them from attacks. HBGary used to perform this kind of service, until it was ambushed. These mercenaries conduct surveillance on the Internet chat rooms where Anonymous hackers congregate, hoping to warn corporate clients of potential peril. They also develop virtual weapons that companies can buy to defend themselves.

It is hard to defend against the media, however, which has mainly served the purposes of Anonymous. One Fortune 100 mercenary I spoke with laid out the typical template in the press:

"The stories are: Insert high-value target here; something bad happens; attribute it to Anon. And people are eating that up." At the "Whoever Fights Monsters" panel discussion in Las Vegas last summer, Joshua Corman says, one hacker in the audience asked, "Why doesn't Anonymous do something more discreet instead of these huge attacks that cause collateral damage, and just tell the press what you did?" Another hacker, who is known to participate in Anonymous operations, answered instantly: "They don't cover it. We tried." Listening to that exchange, Corman says, he realized, "The media is a player in this drama. They're not observing or describing. They're being played."

And they're being played by all parties. The bust of Anonymous and LulzSec in March was hailed even by many leading cyber--security bloggers as "the end of Anon." The idea that any faction of Anonymous has a "head" that could be chopped off, as the F.B.I. claimed, suggests either a fundamental lack of understanding of the phenomenon or a willful misrepresentation of it. (It may well be the latter. According to the F.B.I., the most prominent among the hackers who were arrested, Hector Monsegur, known as "Sabu," had been an F.B.I. informant since the previous June—a period during which he rallied LulzSec hackers to attack the F.B.I.) Corman says, "Even if every current participant of Anonymous were arrested, someone would take up the design of this activity, if not the mantle." In other words: as an instrument of disruption, Anonymous may be too resilient ever to be killed.

V. Organized Chaos

A new telecom treaty is unlikely to result in either side achieving total victory. At the very least, however, the negotiation in Dubai will move countries to put their cards on the table and declare just how much control they want to assert over Internet governance.

The Net has given more individuals more power in a shorter period of time than any new technology in history. And unlike many other world-changing technologies, there is no institutional barrier to access. This has made it, on balance, mostly destructive of institutional authority, especially that of nation-states. National sovereignty encompasses many powers, but one of its core elements has been a monopoly on the control of overwhelming force. Now that hackers are able to penetrate any and all computer networks, including military ones, that monopoly no longer exists. Nation-states, not surprisingly, resist the erosion of their power and seek ways to reclaim it.

Hamadoun Touré, who will be running the show in Dubai, says he seeks nothing more than a "light touch" on the Internet's operations. He in fact chuckled when he uttered those words in the course of an interview.

At least three big issues are very likely to be on the table in Dubai, and there's nothing light about them. One is taxation—a "per click" levy on international Internet traffic. Western countries and business organizations oppose such a tax, as you would expect. China and many Third World countries favor it, saying the funds would help build the Internet in developing countries.

A second issue is data privacy and cyber-security. Authoritarian governments want to tie people's real names and identities to online activity, and they want international law to permit national encryption standards to allow government surveillance.

The third issue is Internet management. Last year, Russia, China, and some pliant allies jointly proposed a U.N. General Assembly resolution (which failed) suggesting the creation of a global information--security "code of conduct" and—as if declaring open season on icann and the other non--governmental groups currently in charge—asserting that "policy authority for Internet-related public issues is the sovereign right of states."

All of these proposals amount to a wish list by the most extreme elements of the forces of Order. The forces of Disorder have no official voice at the negotiations—obviously they're not invited—but they represent a wild card. Although they have thus far shown no apparent interest in Dubai, some of them have announced plans to perform a technical feat beyond anything done so far. In what is being called Operation Global Blackout, they want to bring down the Domain Name System itself—and thus halt all Internet traffic completely—with a springtime attack on the root servers, all in the name of protesting "sopa, Wallstreet, our irresponsible leaders, and the beloved bankers who are starving the world for their own selfish needs out of sheer sadistic fun." Whether that happens (or even could happen), the announcement was an obvious warning flag. Internet experts take the threat seriously. Even if it fails, it presages future attempts.

In the War for the Internet, is there a middle way? The forces of Organized Chaos are not an organized group, don't call themselves by any name, and disagree on many points. In what follows, I'm going to try to distill a synthesis of their views.

The commitment that unanimously binds them is to make the Internet as reliable as possible. One leading apostle of reliability is Dan Kaminsky, a security analyst and D.N.S. expert and the head of a new stealth start-up. He is a close friend of Jeff Moss's—and, like Moss, a self-appointed ambassador to Washington. He sometimes opens meetings on the Hill by saying, "There are bad guys on the Internet. Unfortunately, you're helping them." He is a serial entrepreneur whose current mission is to augment passwords with other ways for Internet users to prove their identities that are more robust, easier to use, and harder to crack. "The only thing everyone agrees on," says Kaminsky, "is that the Internet is making everyone money now and it's got to keep working."

As they devise new systems of authentication, Kaminsky and others are working to be sure that these authentication systems preserve the qualities of privacy and online anonymity—even though anonymity has contributed to, if not created, almost every problem at issue in the War for the Internet. The task at hand is finding some way to square the circle: a way to have both anonymity and authentication—and therefore both generative chaos and the capacity for control—without absolute insistence on either. It is a neat philosophical trick: Sun Tzu meets John Locke meets Adam Smith meets Michel Foucault.

No one can say exactly how these sorts of standards would be defined and applied, or who would be their custodians. World governance doesn't work. It has been pursued for eons by hardheaded pragmatists and woolly-brained eccentrics. Time and again it has been defeated by the vagaries of human nature and the opportunistic conflict of competing interests. In the case of the Internet, the number of interested parties runs into the billions, and they come from divergent cultures and pursue irreconcilable objectives. As Vint Cerf points out, this basic reality seeps through every aspect of the War for the Internet. Around the world and across generations, people have different tolerances for civility, incivility, and invasion of privacy. "I think it will be very hard to resolve this in a way that's globally acceptable," he says.

Freedom in human society, by definition, includes some concept of bound-a-ries. Freedom on the Internet has, thus far, lacked any real concept of boundaries. But boundaries are being invented. It seems certain that nations, corporations, or both will create more zones on the Internet where all who enter will have to prove their real-world identities. Google and Facebook are already moving in this direction. The most heavy-handed suggestions entail a virtual passport or ID, which could include biometric data.

Some see stringent, universal, and mandatory authentication of identity as a commonsense solution to a number of the Internet's biggest problems. If all of our alter egos were brought into line with our analog selves, wouldn't we all behave better? Wouldn't online criminals stop using the cloak of anonymity to steal from and spy on people? Wouldn't people pay for the books, music, movies, and newspapers that many now take for free?

The forces of Organized Chaos reject this argument. Vint Cerf says, “When I hear senators and congressmen complaining about anonymous speech, I want to stop them and say, you should read your own history. The anonymous tracts that objected to British rule and rules had a great deal to do with the American Revolution. Weren’t you paying attention in civics?”

Given the radically decentralized nature of the Internet, the most important thing that anyone can do is to try to make the center hold—but not too tightly. That means protecting the Domain Name System, the Internet’s sole central feature, from government control while keeping governments involved in maintaining it. The point is: there is no single “safe pair of hands,” whatever the forces of Order might say. Any safe pair of hands is a dangerous pair of hands.

At the same time, the security of the D.N.S. itself needs to be radically upgraded, to obstruct hijacking and surveillance. Software-coding languages must become more secure, to make programs more difficult to hack and manipulate. Breach-reporting standards must be established, at least for critical infrastructure, to help corporations and law enforcement share knowledge about hacking threats. Metrics for security and privacy—two qualities that most people value but no one knows how to measure—need to be defined. Finally, “network neutrality” must be preserved. Net neutrality is almost as plastic a concept as Internet freedom, but to the forces of Organized Chaos, it means maintaining the telecommunications infrastructure as a level playing field. The Internet is open to everyone; service providers can’t discriminate; all applications and content moves at the same speed.

To accomplish any of these things, governments will need to create formal mechanisms to give the people who know the most about the Internet—including computer engineers and hackers—a meaningful voice in making policy. Basic Internet literacy is now as critical to good governance as basic knowledge about economics or public health, yet Washington is still full of what Congresswoman Zoe Lofgren, of California, calls “Wite-Out-on-the-screen people.” Dan Kaminsky says that hackers, for their part, have to stop focusing exclusively on “breaking stuff ” and also start focusing on “fixing stuff.”

And if Internet companies do not want intrusive regulation, whether from their own governments or from treaties such as the one to be negotiated in Dubai, they will need to start solving the Internet’s problems on their own. Melissa Hathaway, who led cyber--security strategy for Presidents George W. Bush and Barack Obama, points out that “the top 20 Internet service providers in the world carry 90 percent of the Internet traffic. They can see when you’re infected by a botnet. They can see when you’ve been hacked.” Hathaway has defined a set of general principles that Internet companies and governments might get behind, such as a “duty to warn if in imminent danger.” As she puts it, “It’s just like the law of the sea: the duty to assist.”

Beyond this core agenda, the forces of Organized Chaos, by and large, think that the Internet should be allowed to evolve on its own, the way human societies always have. The forces of Organized Chaos have a pretty good sense of how it will evolve, at least in the short term. The Internet will stratify, as cities did long ago. There will be the mass Internet we already know—a teeming bazaar of artists and merchants and thinkers as well as pickpockets and hucksters and whores. It is a place anyone can enter, anonymously or not, and for free. Travel at your own risk! But anyone who wishes can decide to leave this bazaar for the security of the bank or the government office—or, if you have enough money, the limousine, the Sky Club, the platinum concierge. You will always have to give something up. If you want utter and absolute privacy, you will have to pay for it—or know the right people, who will give you access to their hidden darknets. For some services, you may decide to trade your privacy and anonymity for security. Depending on circumstance and desire, people will range among these worlds.

Aside from wealth or arcane knowledge, the only other guarantor of security will be isolation. Some people will pioneer new ways of life that minimize their involvement online. Still others will opt out altogether—to find or create a little corner of the planet where the Internet does not reach. Depending on how things go, that little corner could become a very crowded place. And you’d be surprised at how many of the best-informed people about the Internet have already started preparing for the trip.