O'REILLY®

Who Are the Bad Guys and What Do They Want?

Gregory Fell
& Mike Barlow

Who Are the Bad Guys and What Do They Want?

Gregory Fell and Mike Barlow

Beijing • Boston • Farnham • Sebastopol • Tokyo O'REILLY®

Who Are the Bad Guys and What Do They Want?

by Gregory Fell and Mike Barlow

Printed in the United States of America.

Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.

O'Reilly books may be purchased for educational, business, or sales promotional use. Online editions are also available for most titles (*http://safaribooksonline.com*). For more information, contact our corporate/institutional sales department: 800-998-9938 or *corporate@oreilly.com*.

Editor: Courtney Allen
Production Editor: Nicholas Adams
Interior Designer: David Futato
Cover Designer: Randy Comer
Illustrator: Rebecca Demarest

March 2016: First Edition

Revision History for the First Edition

2016-03-08: First Release

While the publisher and the authors have used good faith efforts to ensure that the information and instructions contained in this work are accurate, the publisher and the authors disclaim all responsibility for errors or omissions, including without limitation responsibility for damages resulting from the use of or reliance on this work. Use of the information and instructions contained in this work is at your own risk. If any code samples or other technology this work contains or describes is subject to open source licenses or the intellectual property rights of others, it is your responsibility to ensure that your use thereof complies with such licenses and/or rights.

978-1-491-94324-3

[LSI]

Table of Contents

Who Are the Bad Guys?

Cyber Crime Has Many Faces; Understanding Risk is Critical to Implementing Effective Defensive Strategies

In the 1937 movie *Pépé le Moko*, the title character is a Parisian gangster hiding in the Casbah, a "city within a city" in Algiers. For Pépé, the Casbah offers many advantages. Its narrow winding streets look eerily similar, making it difficult for his pursuers to find him. The streets have no names and his pursuers have no accurate maps, a situation that Pépé exploits to elude capture.

Pépé's strategy has become the model for modern cyber criminals. Sometimes their Casbahs are real places, such as Ukraine or Taiwan. Many hide in the Dark Net or behind vast robot networks of hacked computers loaded with malware.

Sometimes, they hide right under our noses: a coworker at a nearby desk, a high school student, or just some random person with a laptop at the local coffee shop. Although most cyber crime is intentional, it's often committed accidentally. Clicking on what appears to be an innocuous link in an email from a friend or simply failing to exercise good password discipline can open doors for cyber criminals and their associates.

Cyber crime and cyber espionage cost the global economy between $375 billion and about $575 billion annually, according to a report issued by the Center for Strategic and International Studies, a Washington think tank. As noted in a Washington Post article, that's far less than the estimates offered by some politicians, but it’s still hefty enough to account for roughly 1 percent of global income.

In addition to its economic impact, cyber crime has become a weapon of terrorist groups and nation states, raising the potential danger to truly nightmarish levels.

Brian Krebs, author of *Spam Nation* and editor of KrebsOnSecurity.com, paints a frightening portrait of organized international cyber crime gangs operating with a sense of entitlement and impunity that would make Al Capone jealous.

Part of the problem stems from what former FBI Assistant Special Agent in Charge John Iannarelli called “breach fatigue” and the general sense that cyber crime is “someone else’s responsibility.” Iannarelli, who now runs a cyber security consultancy, said the readiness of banks and credit card companies to limit losses for consumers hit by fraud creates a false sense of security.

“As a result, most people think that cyber fraud is not a big deal,” he said. “The losses are enormous, but they’re passed along. All of us are paying for them, whether we realize it or not.”

Since the media tends to focus on the most exotic or outrageous forms of cyber crime, most people are unaware that cyber criminals rely heavily on spam to mount successful attacks. Many attacks come in through the front door, in the form of spam disguised as legitimate email.[1]

“For most companies, the best defense is training employees to recognize cyber threats,” said Iannarelli. “People need to learn to spot phishing, whaling, and ‘social engineering’ attacks in which cyber criminals attempt to gain confidential information such as passwords by posing as friends or colleagues.”

Training, however, costs money, and most businesses are reluctant to spend money on activities that don’t help the bottom line. “We’re not all singing from the same sheet of music yet,” he said. “People need to understand the value of protecting themselves from cyber crime. There was a time when people didn’t have locks on their

[1] The APWG, a worldwide coalition of more than 2,000 member organizations, reported 197,252 unique phishing attempts were made in the fourth quarter of 2014, up 18 percent from the previous quarter.

doors. Then they realized locks would protect them and they began buying locks. We're rapidly approaching a similar stage with cyber crime."

Labels Obscure Intent

Seeing the issue as a binary conflict between "good guys in white hats versus bad guys in black hats" can obscure the depth and variety of cyber crime. Richard Moore is managing director at Alvarez & Marsal, a global professional services firm. Prior to joining A&M, he served as head of information security at the New York Life Insurance Company.

From Moore's perspective, applying the "bad guy" label too broadly can lead to oversimplifications, which in turn lead to false assumptions that actually impede or derail investigations. "When we remove the labels, we can see the intent more clearly," he wrote in an email.

Sometimes the intent is reducing the time it takes to conduct research. Other times the intent is revenge. In some instances, the intent is old-fashioned greed. In many cases, however, there is no intent. Some cyber breaches result from accidental errors—the so-called "fat finger" mistakes in which someone types the wrong command or enters the wrong data into a field.

Understanding the intent—or lack of intent—behind a cyber crime is essential to preventing it. Indiscriminately using the "bad guy" label generates F-E-A-R, which stands for "false evidence appearing real," Moore wrote.

In cases of industrial espionage, for example, the actors can be insiders with a grudge or criminals with clients seeking a competitive advantage. Since criminals often rely on insiders, many cyber crimes involve combinations of actors. Terror groups might rely on ad hoc combinations of hackers, insiders, criminals, and even state-sponsored organizations.

Table 1-1 shows the variety of actors, risk vectors, and targets involved in modern cyber conflict.

Table 1-1. Cyber conflict taxonomy

Types of Actors	Examples	Scale of Operations	Intent and Objectives	Scale of Potential Damage	Likely Risk Vectors	Likely Targets
Hacktivists	Anonymous, WikiLeaks, CyberBerkut, Chrysler-Jeep hack	Individuals and small groups	Social/ economic/political change, revenge, greed, sabotage, propaganda, amusement	$ thousands to low millions	DDoS, broken and/or insecure software, insiders	Corporations, schools, government agencies
Insiders	Snowden, Manning	Individuals and small groups	Theft and/or exfiltration of IP, sabotage	$ thousands to high millions	Internal systems (i.e., financial, HR, manufacturing)	Corporations, schools, government agencies, financial institutions
Criminals	Condor, Coolio, T33kid, Kwyjibo	Individuals, small groups, organized gangs and syndicates	Extortion, theft and/or exfiltration of IP (PII, PHI, clickstream data), sabotage	$ millions to low billions	Email phishing, SQL injection, DDoS, broken and/or insecure software, insiders	Corporations, schools, government agencies, financial institutions
Terrorists	ISIL, al-Qaeda	Small groups, organized gangs, and global networks	Propaganda, relay instructions to field operatives, extortion, monitor enemies	$ millions to high billions	Social media, insiders	"Soft targets" (e.g., schools, public spaces, sports arenas, transportation hubs, airlines)
Nations	US, China, Russia, Israel, Iran, France	Specialized teams, military units, and government agencies	Destabilize/destroy military and civil infrastructure control systems, monitor, and/or disrupt enemy communications	$ trillions and upwards	Broken and/or insecure software, insiders, spies	Critical infrastructure, (e.g., roads, bridges, airports, hospitals, utility grids, water systems), military installations

The landscape of cyber conflict is complex and varied. Moreover, the relationships between actors, operations, scale, and risk vectors aren't linear. Amateur hackers are capable of inflicting as much—and sometimes even more—damage than professionals. Many hackers now consider themselves "security researchers" whose work is essential to the continuing health of the cyber economy. Some argue that it's important to make a distinction between "cyber hackers" and "cyber attackers."

Although the table suggests an orderly hierarchy within a stable community of cyber combatants, the real-world relationships are less like rigid hierarchies and more like networks or ecosystems as in Figure 1-1.

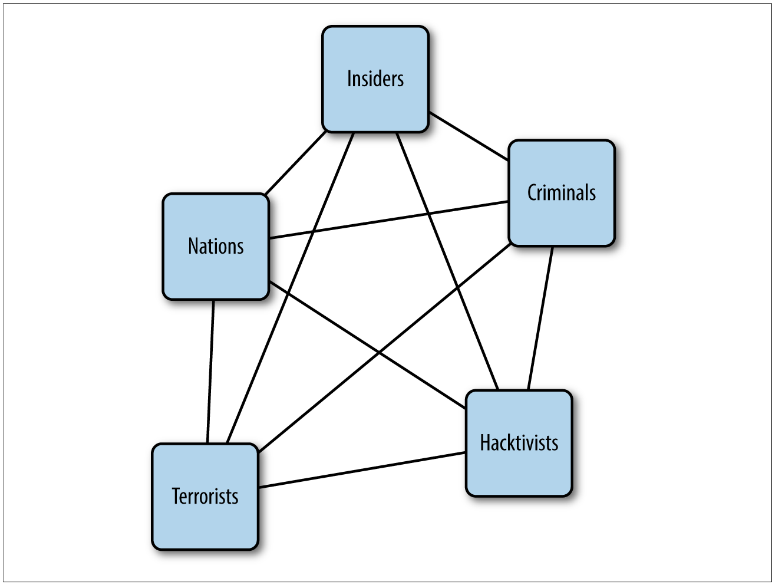

Figure 1-1. In cyber crime, relationships between various actors are more like networks than structured hierarchies

The good news is that no single country or gang can lay claim to being the most powerful player in 21st century cyber conflict—at least not yet. The bad news is that because cyber criminals don't have capitals or headquarters, they are hard to eradicate.

Accidents Happen

As mentioned earlier, many cyber incidents result from accidents—so essentially, they are part of human nature. In some instances, hackers manage to damage systems and corrupt data without realizing the extent of the harm they've caused. That said, there's a substantive difference between teenagers hacking for kicks, criminals hacking for money, and spies hacking for foreign governments.

"Today's kids grow up with computers and they develop hacking capabilities," said Pete Herzog, cofounder of the Institute for Security and Open Methodologies (ISECOM) and cofounder of Hacker Highschool, which provides teens with hands-on lessons designed specifically to help them learn cyber security and critical Internet skills.

When teens are frustrated and lash out, they often turn to the closest tools available—which in many cases are PCs or laptops. "If they're caught breaking a window or knocking over a mailbox, they get a warning. But if they're caught hacking, we send them to jail. That makes no sense to me," Herzog said.

Not all cyber attackers have malicious motivations, said Justine Bone, a cyber security consultant. "More often than not, hackers are driven by curiosity, a desire to learn more about how a system works. Usually this involves subverting the intended behavior of a system."

Bone has been described as "classical ballerina-turned hacker-turned CISO." She is currently executive director of Secured Worldwide, a "stealth startup" focused on wireless encryption and packaging technology used for decentralized global trading.

Most hackers are not driven by the urge to steal data or damage systems, she said. "It's the folks with malicious motivations who are the real bad guys ... the people who want power, money, or inside information ... or who want to create chaos and are prepared to go to any lengths to achieve their goals."

50 Shades of Cyber Crime

Cyber crimes are committed by a broad range of people and organizations, which makes it difficult to offer a uniform description of a “typical” cyber criminal and virtually impossible to concoct a “magic bullet” that would work effectively in a variety of situations.

“The real answer is the bad guys are going to be different according to who you are and what you’re trying to protect,” said Gary McGraw, the chief technology officer at Cigital, a software security consulting firm. For example, cyber criminals who target financial services companies operate differently than cyber criminals who target industrial companies. “You need to consider all the categories of cyber crime and determine how they impact you. Everybody may have a different set of threats they have to deal with. Effective security is a very context-sensitive set of decisions.”

McGraw sees cyber security as a risk management problem. Instead of grasping for technology solutions, organizations should take the time to qualify and quantify the cyber security risks facing them, and then devise specific policies and processes for eliminating or mitigating those risks.

He is also a true believer in the concept of maintaining a strong defense against cyber criminals. Too often, he said, cyber offense takes precedence over cyber defense. That’s natural because playing offense always seems more exciting and generates more attention than playing defense. But cyber crime isn’t like sports. Despite the attention garnered by successful offensive tactics such as the Stuxnet virus, which slowed down the Iranian nuclear program, a solid defense is the best strategy for thwarting cyber “bad guys”—at least for the foreseeable future.

“The NSA (National Security Agency) is pretty good at playing offense,” said McGraw. “But the notion of throwing rocks seems great until you realize those rocks can be thrown back at you. We live in glass houses, and people who live in glass houses shouldn’t throw rocks.”

From McGraw’s point of view, the underlying challenge is building better and more secure software. “The biggest risk vector is software. Broken software is our Achilles heel,” he said.

The Soft Underbelly of Cyber Security

If software itself can be considered an attack surface, then we’re all in trouble. Achilles’ heel was his only weak spot; the rest of him was invulnerable. Software, on the other hand, is everywhere.

“Software vulnerabilities are an arms race. Bugs are found, bugs are exploited, bugs are fixed, repeat. No software is written perfectly,” said Bone. “In addition, changing approaches to software development practices such as Agile and DevOps have raised the bar for security engineers. Automated security assessment has not kept pace with automated software development and deployment practices, and the delta is dangerous. Technology risk managers must be careful to understand and communicate the impact of this issue as those software development philosophies become more widely adopted.”

Bone also sees cyber security as “a risk management issue, and risk management is an art. This is beginning to be recognized at more progressive companies, where we see changing security governance models.”

Generally, however, those governance models tend to change slowly. “Once upon a time, information security was considered a subset of the overall technology program, and your security head reported into the CTO or CIO’s organization,” she wrote.

But the security heads—also known as chief information security officers or CISOs—had limited insight into the businesses they worked for. As a result, according to Bone, “the business gets frustrated by unrealistic demands from the CISO that negatively impact business processes and opportunities ... and the CISO, who is primarily a technology expert, gets frustrated because he or she doesn’t understand the business priorities.”

In the eyes of some experts, effective cyber security requires a new cultural mindset. Companies need to accept and embrace cyber security as a strategic competency, much as they have learned to accept and embrace the concept of customer-centricity, an idea that was initially ridiculed but is now considered an essential component of business strategy.

“Cyber security involves people, process, and technology. We need to address key areas of each of those categories in order to create a secure environment and maintain a secure environment,” said Nate Kube, chief technology officer, cyber security at GE and founder of Wurldtech Security Technologies, a GE subsidiary. “We need education for people, strong processes around password management ... and technologies that are updatable for security risk.”

Models for Change

A body of work focused on establishing common language and defining new models for managing cyber security is emerging from the chaos. Working with the Carnegie Mellon University Software Engineering Institute, the US Department of Energy (DOE) has developed the Cybersecurity Capability Maturity Model (C2M2). The C2M2 is based on Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) developed "in partnership with the Department of Homeland Security, and in collaboration with private- and public-sector experts," according the DOE.

McGraw, with coauthors Sammy Migues and Jacob West, have written Building Security in Maturity Model Version 6 (BSIMM6), a document based on a multiyear study "built directly out of data observed in 78 software security initiatives from firms including: Adobe, Aetna, ANDA, Autodesk, Bank of America, Black Knight Financial Services, BMO Financial Group, Box, Capital One, Cisco, Citigroup, Comerica, Cryptography Research, Depository Trust and Clearing Corporation, Elavon, EMC, Epsilon, Experian, Fannie Mae, Fidelity, F-Secure, HP Fortify, HSBC, Intel Security, JPMorgan Chase & Co., Lenovo, LinkedIn, Marks & Spencer, McKesson, NetApp, NetSuite, Neustar, Nokia, NVIDIA, PayPal, Pearson Learning Technologies, Qualcomm, Rackspace, Salesforce, Siemens, Sony Mobile, Symantec, The Advisory Board, The Home Depot, Tom-Tom, Trainline, U.S. Bank, Vanguard, Visa, VMware, Wells Fargo, and Zephyr Health."

BSIMM6 is intended as a "measuring stick for software security," according to its authors. Additionally, it shows "how mature software security initiatives evolve, change, and improve over time."

Indeed, one of the key takeaways from the BSIMM6 is the evolving nature of the risk landscape. Perhaps that's one reason why McGraw emphasizes the need for strong defenses. "We don't know who does what on the Internet," he said. "There is a real attribution problem. We cannot say precisely who is behind every cyber attack ... Our vulnerabilities are pervasive."

In a recent article, Herzog described the dilemma facing all cyber security professionals: "One day, you're reading the news ... and you find an article on how to perfectly secure your data in three easy steps. It says put up a firewall, install antivirus on all your machines, and use 24/7 automated updating and patching. You laugh out loud and water comes out your nose."

Designing Security Into Software and Systems

How useful is cryptography in solving cyber security issues? Most experts agree that while it can be highly useful, it's not the complete solution.

"The idea that you can sprinkle magic crypto fairy dust liberally around your software and it will be secure is wrong on many levels. First of all, security is a system property, not a thing. So adding a thing to your code is unlikely to make it secure. Secondly, cryptography is mind bogglingly hard to get right. Not only is the math difficult, applied cryptography is riddled with massive sneaky pitfalls that are easy to get wrong," McGraw wrote in a post titled "Seven myths of software security best practices."

McGraw's main message to developers is simple: Build security into software from the get-go. "Software security is about integrating security practices into the way you build software, not integrating security features into your code," he wrote.

"You need to start thinking about security when you're in the early design stage, before you write a single line of code, when you're architecting the system," said Kube. "You have to take into consideration where the software is going to be installed and what the use cases are. Then you need to look at the exposures for those particular use cases from the standpoint of physical, digital, and network access."

Even if every line of code could somehow be made secure, there's no guarantee that cyber crime would simply vanish. "There's always another way to breach a network," said Jeffrey Carr, a security consultant specializing in cyber warfare strategy and tactics. "The surest and easiest ways are through supply chains and employees."

Carr is the author of *Inside Cyber Warfare: Mapping the Cyber Underworld* (O'Reilly) and numerous blog posts on cyber topics. "I don't like to use the term 'bad guys,' since good and bad are relative and easily interchangeable among actors, including us. I prefer 'rivals' or 'adversaries'—and they could be anyone," said Carr.

Hacking the Internet of Things

Whether you call them "good guys" or "bad guys," this much is certain: For hackers, the best days are ahead. The expanding Internet of Things (IoT) offers vast opportunities for hackers bent on making mischief. At least in the past, hackers were relegated to operating within computer systems and data networks. When the IoT kicks into high gear, determined hackers will have access to billions of connected devices at all levels of society.

"You can tell when someone in their home takes a bath or a shower, or goes to the bathroom, simply by monitoring a single pressure measurement device," said Augustin Chaintreau, an assistant professor in the Computer Science Department at Columbia University and a member of the university's Data Science Institute. "It's amazing how much can be learned about someone's lifestyle by mining information on energy consumption and movement."

As the IoT permeates more areas of daily life, Chaintreau and his colleagues are concerned about "information leakage" from seemingly "benign monitoring" of physical systems such as water tanks, air conditioners, and heating plants.

The potential for harm grows enormously as the IoT penetrates industry, manufacturing, and utilities. Although a handful of cyber security firms have turned their attention to the IoT and its larger cousin, the Industrial Internet, an unhealthy schism has developed between the cultures of information technology (IT) and operational technology (OT).

The OT community doesn't trust the IT community to provide genuinely secure solutions. The common OT argument goes something like this: "If IT can't protect credit card information from hackers, how can we expect it to protect real assets such as power grids, energy plants, municipal water systems, and transportation networks?"

The IT community, on the other hand, argues that its experience managing highly complex enterprise systems creates a major advantage that can be used to fight a wide variety of cyber criminals.

"The trust gap between IT and OT can be enormous," said Francis Cianfrocca, founder and chief executive officer of Bayshore Networks, a firm specializing in cyber security for the IoT. “It’s a serious problem we have to solve.”

A common misconception among OT is that their facilities are immune from Internet hackers. With the exception of the nuclear industry, which has taken extreme measures to isolate its systems, most of the world’s industrial and manufacturing facilities are already connected to the Internet. “Every place you go, you will find wireless access points, which are the easiest targets for hackers,” Cianfrocca said. “So the bottom line is many facilities are vulnerable, and their operators aren’t admitting it, or they don’t know.”

IT people and OT people look at the world differently, said Jesus Molina, a security consultant for Fujitsu. IT people focus on security, which they define as protecting systems from the environment. OT people focus on safety, which they define as protecting the environment from systems, he said.

“With OT, the first priority is safety and the second priority is reliability,” he said. As a result, OT practitioners often resist shutting down systems, even when the software in those systems requires upgrades or patches.

The divergent philosophies of IT and OT make it difficult to simply “merge” cyber security solutions and to create practical integrated strategies for managing risk. “Complex software can never be entirely free of errors,” Kube said. “How do you manage the risk without taking systems offline?”

Cianfrocca sees an emerging field of “cyber hardening,” in which military and industrial assets are designed to be more resilient to cyber attacks. Defense contractors such as Raytheon, for example, are building anti-hacking systems into connected devices that would prevent them from being commandeered by unauthorized operators.

Raytheon recommends four basic steps that any organization can take to protect assets from cyber attackers:

1. Conduct vulnerability assessments and penetration testing of hardware and software;
2. Update outdated and unpatched software, remove unnecessary software, and delete old user accounts;

3. Set up intrusion detection, intrusion prevention, and tamper resistant protections;
4. Make sure supply chain partners employ strong cyber hardening practices.

“Cyber hardening helps reduce a system’s vulnerability surface. In other words, it can limit or eliminate security holes hackers could use to penetrate systems and cause harm,” according to Raytheon’s website.

Slippery Slopes

Walt Kelly, the creator of “Pogo,” famously wrote, “We have met the enemy and he is us.” Several of the experts interviewed for this report said increasing levels of surveillance and interference by governments and their agencies pose far deeper threats to modern society than haphazard acts of hacking committed by terrorists or criminal gangs. Some governments already make a practice of restricting Internet access during times of civil unrest. That hasn’t happened in the United States—yet.

“I trust the people leading the NSA and US Cyber Command today. But those people won’t be there forever and there’s no guarantee their successors will have the same commitment to protecting our freedoms,” Cianfrocca said. “The challenge for us is discerning whether the government is acting to protect us or to protect itself.” Since governments “are very good at keeping secrets,” he said, it will be hard for ordinary citizens to know when the line has been crossed.

As our lives become a blend of physical and digital experiences, cyber crime has emerged as a new kind of social disease. We don’t know yet whether this disease is chronic or acute, but there’s no denying its existence. Rather than labeling one set of hackers as “good guys” and another as “bad guys,” we should focus on devising the best strategies for managing risk over the long term and defending ourselves against outright harm in the short term.

“Cyber risk management” might not sound as cool as “cyber warfare,” but it might be the best way for treating a disease that isn’t likely to go away anytime soon.

About the Authors

Greg Fell is a general partner in The Investors Collaborative, a Boston-based venture capital group. He is the former chief strategy officer at Crisply, an enterprise SaaS company that pioneered the algorithmic quantification of work. Previously, he served as vice president and chief information officer of Terex Corp., a global manufacturer of industrial equipment.

Before joining Terex, Fell spent nearly 20 years with Ford Motor Company. He started as a developer, and worked his way through a variety of management roles supporting the global Engineering and Manufacturing functions of the company. He has domain expertise on CAD/CAM/CAE systems, lean manufacturing, and control systems.

Fell is a graduate of Michigan State University, and spent several years on staff in the College of Engineering as a Senior Research Programmer and Instructor.

Fell is active in the CIO community. He is the former Chairman of the Fairfield Westchester Society of Information Managers, a former Board Member with Junior Achievement, and has mentored high school students through the First Tee Program.

His book, *Decoding the IT Value Problem* (Wiley, 2013), is used widely by CIOs to calculate the economic value of IT projects.

Mike Barlow is an award-winning journalist, author, and communications strategy consultant. Since launching his own firm, Cumulus Partners, he has worked with various organizations in numerous industries.

Barlow is the author of *Learning to Love Data Science* (O'Reilly, 2015). He is the coauthor of *The Executive's Guide to Enterprise Social Media Strategy* (Wiley, 2011) and *Partnering with the CIO: The Future of IT Sales Seen Through the Eyes of Key Decision Makers* (Wiley, 2007). He is also the writer of many articles, reports, and white papers on numerous topics such as collaborative social networking, cloud computing, IT infrastructure, predictive maintenance, data analytics, and data visualization.

Over the course of a long career, Barlow was a reporter and editor at several respected suburban daily newspapers, including the *Journal*

News and the *Stamford Advocate*. His feature stories and columns appeared regularly in the *Los Angeles Times*, *Chicago Tribune*, *Miami Herald*, *Newsday* and other major US dailies. He has also written extensively for O'Reilly Media.

A graduate of Hamilton College, he is a licensed private pilot, avid reader and enthusiastic ice hockey fan.