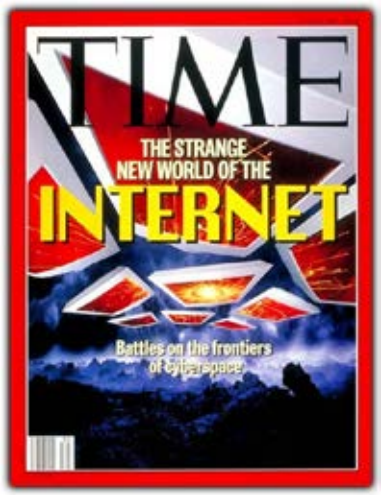
Using Recombinant Innovation for Post Cyber-Strike Recovery Means

By LtCol John Dobrydney, U.S. Marine Corps, CISSP, Contributing Editor

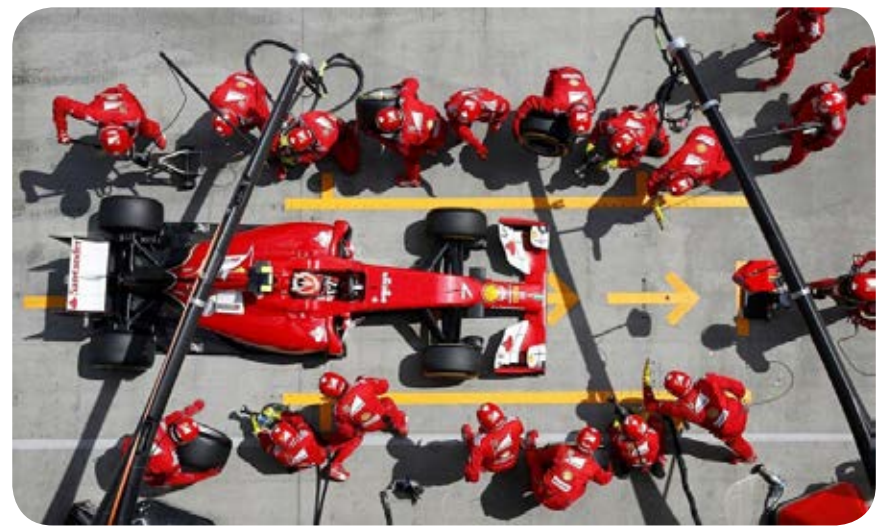


Time Magazine Cover from 1994

The early 1990s provided the fastest and, in a sense, the most efficient means of providing goods and services – the Internet operationalized through the World Wide Web (WWW) for the average user. Moving electrons at near light speed from almost anywhere in the world provides virtually unlimited access to information and Internet-provided goods and services to any other part of the world. Internet-provided services scale from the individual user to all levels of government to international communities of governance, economic alliances, and security organizations. Once realized, governments, industry, and society embraced the Internet's speed, convenience, and universality: the WWW, through the Internet, provided a means to satisfy a growing list of unlimited wants and needs. However, the Internet was designed for accessibility, not security, making it easily vulnerable to service degradation, disruption, and possible destruction. A successful large-scale cyber strike against the United States could cause widespread service disruptions across all governance, societal, and economic sectors due to the Internet's inherent interconnected nature. As "most everything" is connected to "most everything else", post-strike effects will cascade with varying degrees of impact across the network, interfering with network performance as well as the governing, societal, and business operations and processes relying on the network. These cascading disruptions will have second and third order effects as they spill over to the physical world. Warding off the systemic physical world disruptions requires innovative methods to stabilize and then restore both Internet-provided services and the government, economic, and social functions relying on the Internet. Should a crippling cyber strike launched against the United States' government, military, economic and societal infrastructure occur, "recombinant innovation" executed in a decentralized manner provides a means to rapidly and creatively solve the challenges of rebuilding society and restoring critical services and return the United States to an acceptable recovery and productivity trajectory.

"A rationally acting person desires to satisfy unlimited wants and needs" is a foundational economic principle. The problem is how to best allocate scarce resources, or means, against those unlimited wants and needs so as to satisfy the greatest number of people. Means come in many forms and can be defined according to the desired ends: money brings entertainment, food provides fuel for energy, exercise promotes health and well-being, labor provides compensation, and education leads to innovation. As technology progresses, innovators learn to incorporate new means to satisfy their ends – in some cases by producing something new by recombining existing technology or processes, a technique known as recombinant innovation.

Examples of recombinant innovation abound. One involves the unlikely combination of surgeons and Formula One pit crews: "Surgeons at a London children's hospital became aware of the similarities between the handover disciplines from theatre to intensive care and what they saw in the pit of a Formula One racing team."[1] By noticing the similarities the surgeons recognized a useful practice that they could incorporate into their emergency room procedures. Pit crews are highly orchestrated. Each person performs a very specific task at a specific time and in a specific sequence in concert with every other person on the team. The result is maximum work done in a minimum amount of time within extremely high performance standards. The surgical team adopted the same approach to their procedures and reduced the time it took to train a new team to a high standard of proficiency.[2]



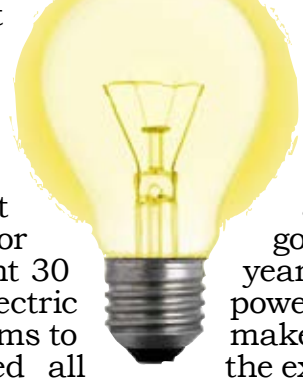
RECOMBINANT INNOVATION

A more recognizable example of recombinant innovation is "sampling", a very common practice that arose during the advent of digital music technology in the 1980s.[3]

Artists combine melodies from other songs and incorporate them into their own - a recent example being Robin Thicke's "Blurred Lines" which heavily borrowed from Marvin Gaye's "Got to Give it Up." In the business world, innovators created e-commerce by combining a company's already existing database with a "front-end" interface on the WWW that a user could access via a web browser. Producers and retailers could offer goods and services to a much wider audience at a fraction of the advertising, shipping, and storage costs. Other innovators created Intelligence, Surveillance, and Reconnaissance (ISR) satellites by combining a rocket with a radio, a chassis, and a camera. A Virtual Machine (VM), software that creates multiple servers instantiated on a single hardware computer, is a combination of software and Moore's Law. One might even argue that the Internet itself is a product of Recombinant Innovation: electricity, logic, and openly available protocols. These are but a few examples; the possibilities of recombinant innovation are virtually limitless. As the authors of The Second Machine Age point out "if there were only 52 seed ideas in such an economy, they have many more potential combinations than there are atoms in our solar system."[4]

"Following a cyber strike, recombinant innovation provides a ways to achieve the ends of rapidly recovering and restoring the government and society's access to the good and services provided by the Internet through the means of very incentivized innovators."

Innovation, according to MIT's Erik Brynjolfsson and Andrew McAfee is key: "From an economist's perspective, satisfying these desires is great—taking care of consumer demand is usually seen as a good thing. But innovation is also the most important force that makes our society wealthier."[5] For example, Henry Ford innovated when he introduced the assembly line to automobile manufacturing. His production plants could produce cars faster and at less cost than conventional methods could. The key to Ford's success was that he did not invent anything new. He combined ideas he saw at a meatpacking plant with automobile manufacturing to produce a product that was within financial reach of the average American.[6] Thomas Edison was not really an inventor per se either and "didn't actually invent the light bulb. That honor goes to J. W. Starr, who filed the patent 30 years earlier."[7] Edison "figu[red] out the electric power generation and transmission systems to make it truly useful. So Edison adapted all the existing technology, including Starr's patent, and created the first system of electric lighting. In this way, the "invention" of electric lighting that we take for granted was, in fact, a recombinant innovation."[8] Ford and Edison both found ways to "build innovation strategies around recombining existing technologies rather than inventing new ones."[9]



The Achilles' heel associated with the WWW and the Internet is that its foundational protocol inventors were not initially concerned with security thereby rendering it extremely vulnerable to accidental or malicious threats. The Internet's underlying weakness is the catalyst to potential societal disruption. The United States' economy, which is highly reliant on the Internet, would tank with the right cyber strike combinations and intensity levels.[10] Investors would sell their positions as fast as they can – if the mechanisms exist for them to do so since the financial industry is highly automated. Since the major world economies are interconnected, a panic in the United States will cause economic panic around the world. The systemic network collapse will affect most Americans who have experience with conducting business an "analog" world. Going to a bank to withdraw cash or balance a checkbook, mailing a letter via "snail-mail", going to a travel agent for airline tickets, buying a book at a brick and mortar store, or even reading a map are older and uncommon habits. Likewise, in the military, conducting business and operations via email, "chat", a common operational picture, SharePoint, and auto-deposited paychecks are today's way of life. Semaphore, Morse code, celestial navigation, "yellow canaries", hard checks on payday, and operating with HF radio are fading memories, retained only in the memories of senior leaders and make for great "sea stories". Increasing reliance on the Internet's benefits changed the way governments, the economy, and society operate. Coping in an analog environment and restoring "normal" functioning requires dedicated thought as what is now taken for granted will suddenly become very hard to accomplish.

Several post cyber-strike recovery methods for the United States government, economy, and society are available. The first is top-down and centralized in which the government directs recovery efforts. Since the United States' military, government, economy, and society rely on much of the same Internet it, therefore, it is imperative that Internet cyber security remains a national priority. The recently established Department of Homeland Security (DHS) and United States Cyber Command (CYBERCOM) defend the United States' domestic and military networks respectively. DHS specifically is required to "secure civilian government computer systems, and work with industry and state, local, tribal and territorial governments to secure critical infrastructure and information systems"[11] while CYBERCOM "conducts full-spectrum military cyberspace operations."[12] At the higher governmental level, these organizations' missions make sense; however, it is not the most efficient means to reach the lowest levels of government and society and solve the indirectly related problems, e.g., a data integrity problem that the stock market may experience if it is unknown whether or not a number of transactions completed. Such challenges are best solved by those closest to and most invested in the problem.

Research in disaster recovery shows that "Victims are often themselves the first responders and that centralized, hierarchical, bureaucratic responses can hamper their ability to respond in the decentralized, self-organized manner that has often proved to be more effective."[13] Likewise, "...over the last 50 years, U.S. military doctrine has increasingly identified decentralization, self-organization, and information sharing as the keys to effectively operating in ever-more complex conflicts that move at an ever-faster pace and over ever-greater geographical distances."[14] Therefore, DHS and CYBERCOM are better suited to coordinate and facilitate information sharing and provide resources to those individuals and organizations closer to the problems. Trying to drive the solution from afar, especially when the means of communications are limited or nonexistent, slows the process and stifles the creative energies that naturally arise from motivated rational actors acting in their self-interest. Decentralization, self-organization, and information sharing is a more appropriate post cyber-strike method than a top-down driven, centralized model and better suited to solve the types of problems caused by a cyber attack, and facilitates innovative problem solving. Recombinant innovation, through a decentralized, self-organized, and shared information process provides the means to solve the post-cyber strike challenges government and society will face.

A post-cyber strike strategy to restore Internet services reliant on a common communications model needs to be based on innovating existing technologies vice inventing something completely new. Demand for restoring WWW and Internet-like capabilities will not allow for the time needed for a completely new technology. By using existing resources, the knowledge and expertise already exists thereby negating an extremely steep learning curve derived from trial and error. The "trick" with recombinant innovation is to combine existing resources or processes in heretofore unimagined ways to achieve desired, or even unexpected, means The more that existing resources are reused, the higher the probability of its availability. If networking hardware is part of the recombinant innovative solution then that hardware is already largely in place. Along with resources normally associated with the Internet are the users who rely on the Internet for everyday business operations and understand the IT-supported business processes. This intellectual capital is the most crucial asset, as they best understand the ends from which the products of recombinant innovation aim to achieve.

Recombinant innovation requires a unique organizational approach to produce successful solutions. Empirical evidence shows that "entrepreneurs and [innovators] are no smarter, no more courageous, tenacious, or rebellious than the rest of us. They are simply better connected.... Innovators don't benefit just from deep, intensive teamwork, but from casual connections that lead to chance encounters with unfamiliar ideas"[15]. Forming and encouraging diverse, interdisciplinary groupings the nation can start addressing how to respond to a cyber- strike before it is engulfed in crisis, as well as provide insights on making the nation's information systems more resilient. These innovators can come from subsets of local governments, schools, universities, think tanks, veterans associations, hobby clubs, churches, and any other loosely connected entities to combine and engage in recombinant innovation to solve the problems confronting them. Even getting an eclectic group of people together at the coffee shop with paper notices posted on physical bulletin boards in the absence of a functioning Internet will begin to generate ideas. Recombinant innovative practitioners have found that: "You don't have to rely on independent geniuses. Just put talented, imaginative people in work environments where there is open-minded give and take and a feeling of freedom to introduce the kinds of disruptive ideas that shake up the marketplace and the competition."[16] The resulting innovations need a channel for execution whether locally or filtered to higher levels and require rudimentary planning prior to and will need a solution after the fact if the strike destroyed the means to do so.

Following a cyber strike, recombinant innovation provides a ways to achieve the ends of rapidly recovering and restoring the government and society's access to the good and services provided by the Internet through the means of very incentivized innovators . It can be assumed that high dependence on the Internet and the rational desire to maximize the benefits derived will push government and society to try to recover the status quo ante if not design a network that will resist all but the most extreme attacks. It is also rational to have organization and an implementation plan in place prior to a cyber strike given the know Internet fragilities and almost wholesale dependencies. Local governments, communities, the military, and industries need to work from within and build their contingency plans to support innovative solutions to the as yet unknown problems that will arise. Basic and critical functions such as water, power, banking, and financial market operations require rapid responsiveness to form a solid governmental and societal base from which to tackle the longer-term problems. These problems include fully restoring economic integrity and confidence in the system as well as offensive cyber capability for the military to deter, respond if necessary, and prevent another attack from occurring. Equally as important is designing a more resilient communications model that can either withstand all but the most violent attacks or one that can make such attacks irrelevant.

Innovation produced the Internet; conceivably, innovation could also produce the means to recover from the societal disruption caused by a cyber-strike in a timely and feasible manner. Planning ahead now to actively employ recombinant innovation to solve the known and, more importantly, the unknown challenges that will follow a crippling cyber strike is essential. Government at all levels, federal agencies, segments of industry, and individual citizens need to plan, wargame, and exercise how they will organize and begin to understand, frame, and triage the resulting challenges. Envisioning their innovation problem-solving group composition, determining who they will look for, where they will meet, and how they will execute and communicate their plans will mitigate the strike's second and third order effects and can be thought of as an on-call recovery measure that may also help maintain society's confidence. Employing recombinant innovation and basic economic principles can position a crippled United States for a faster recovery and take advantage of people's natural tendency to rationally act in their best interest.

A Marine Communications Officer, Lieutenant Colonel John Dobrydney is an experienced cybersecurity and network operations planner. He recently served as the Commanding Officer of Marine Wing Communications Squadron – 18, the Executive Officer of 7th Communication Battalion, the Network Operations Officer for the III MEF G6, and served as the Enterprise Information Assurance Branch Head at Headquarters, Marine Corps C4 Directorate. He currently serves as the Cybersecurity Division Chief, Joint Staff J6. Lieutenant Colonel Dobrydney has a Masters of Security Studies from the Marine Corps War College and a Master of Science in IT Management from the Naval Postgraduate School.

1 "Recombinant Innovation," accessed December 8, 2015, http:// www.doorsofperception.com/social-innovation/recombinant-innovation/.
2 ibid.
3 "Sampling Safely – A Primer to Avoiding Lawsuits | Copyright | Legal / Grants," accessed December 12, 2015, http://schoolvideonews.com/Copyright/Sampling-Safely- %E2%80%93-A-Primer-to-Avoiding-Lawsuits.
4 Brynjolfsson, Erick and Andrew McAfee, The Second Machine Age, (New York: W. W, Norton & Company, 2014), 82.
5 Erik Brynjolfsson and Andrew McAfee, "The Innovation Dilemma: Is America Stagnating?," TPM, February 11, 2014, http://talkingpointsmemo.com/cafe/the-innovation- dilemma-is-america-stagnating.
6 "Recombinant Innovation," accessed December 12, 2015, http://www.strategy- business.com/article/04404?gko=282e2.
7 Andrew C. Revkin, "Innovation from the Bottom Up," Dot Earth Blog, accessed December 8, 2015, http://dotearth.blogs.nytimes.com/2011/07/28/innovation-from-the-bottom- up/.
8 ibid.
9 ibid.
10 "Is Economic Armageddon Just 1 Click Away?," WND, accessed December 13, 2015, http://www.wnd.com/2015/07/economy-just-1-click-away-from-catastrophic-meltdown/.
11 "Safeguard and Secure Cyberspace | Homeland Security," accessed December 4, 2015, http://www.dhs.gov/safeguard-and-secure-cyberspace.
12 R. Stone, "A Call to Cyber Arms," Science 339, no. 6123 (March 1, 2013): 1026–27, doi:10.1126/science.339.6123.1026.
13 Sean Lawson, "Beyond Cyber-Doom: Cyberattack Scenarios and the Evidence of History," Mercatus Center at George Mason University, 2011, http://mercatus.org/sites/default/ files/publication/beyond-cyber-doom-cyber-attack-scenarios-evidence-history_1.pdf.
14 ibid.
15 "Recombinant Innovation," Strategy+business, accessed December 6, 2015, http:// www.strategy-business.com/article/04404?gko=282e2.
16 ibid.