

Keynote Remarks for the Cyber Colloquium, Washington, DC
by Dr. Regina E. Dugan, Director, DARPA
7 November 2011

It is the making of novels and poetry. From Dickens to Gibran.ⁱ That the best and the worst occupy the same time. That wisdom and foolishness appear in the same age...light and darkness in the same season. That joy is sorrow unmasked. That humans are suspended like scales between inseparable, contrasting emotions only at standstill and balanced when they feel nothing.

These are the timeless words of our existence. We know it is true. Of everything.

Cyberspace is occupied by humans. As of March 31st of this year, it is occupied by just over 2 billion, or about 30 percent of the world's population.

It should come as no surprise, therefore, that it is occupied by some of the best and some of the worst. By both wisdom and foolishness. Acts of aggression and peaceful protests. By those who have found a new way to have their voice heard, and those intent on suppressing voices that do not echo their own. By a new class of talent, so-called hackers. They are good and bad, expert and novice. By pacifists and warriors. Attackers and defenders. By profound heroism and shocking injustice.

It is a new domain, but it conforms to the timelessness of our existence. We know it is true. Of cyberspace too.

The advent of the internet more than 40 years ago, created both tremendous opportunity and new risks. Today, there are 800 million friends on Facebook... and the emergence of cyberbullying. On a slow day, there are 140 million tweets sent by microbloggers... from mundane musings to hashtagged revolutions. More video is uploaded to YouTube in 60 days than was created in 60 years by the three major U.S. networks combined. Two billion YouTube videos are viewed per day. It's become a new form of art... A feature length film entitled "Life in the Day" is the work of Kevin Macdonald, who asked the people of the world to chronicle a single day in their lives... July 24th, 2010. He received 80,000 submissions and 4,500 hours of footage from 192 countries.

J.P. Morgan reports that worldwide e-commerce sales are expected to increase from \$573 Billion in 2010 to nearly \$1 Trillion in 2013. Each year, cybercriminals and thieves steal terrabytes of data, intellectual property worth billions, expose an average of 260,000 personal identities per data breach, and cost organizations approximately \$7.2M per data breach event. Symantec reported that this past summer, 29 chemical companies, including multiple Fortune 100 companies, were subject to computer attacks that sought to extract data on formulas and manufacturing processes.

It is a thriving industry. Indeed, according to McNiven, a US Treasury advisor on cybercrime, 2004 was the first year that proceeds from cybercrime were greater than

proceeds from the sale of illegal drugs (although the specific numbers are disputed). What is not disputed is that over 30 million new malware variants are discovered each year.

Cyberspace occupants coexist in the physical world. Their virtual- and physical-world identities may be the same. Or not. There are those who seek fame coincident with their physical-world existence... and those who seek the protections of a virtual-world anonymity.

Anonymity is, in and of itself, neither good nor bad. It might be how ideologically dissatisfied, sympathetic people are recruited to reveal information as part of a cause. That information may pose significant ramifications, intended or unintended, for companies, countries, or individuals. It might be how information is revealed about members of a ruthless crime syndicate in Mexico.

The crossover from the virtual world to the physical world is felt in the collapse of financial systems and the resulting lost homes, in political protests that result in death. Malicious cyberattacks are not merely an existential threat to our bits and bytes; they are a real threat to an increasingly large number of systems that we interact with daily from the power grid to our financial systems to our automobiles and our military systems.

The best and the worst; indeed, occupy the same time.

Former Deputy Secretary of Defense Lynn said on September 28, 2011 that *“cyberattacks will be a significant component of future conflicts”* and that *“over thirty countries are creating cyber units in their militaries.”* He argued that, *“it is unrealistic to believe that each one will limit its capabilities to defense.”*

On October 12th, *The Financial Times* reported the Chinese military mobilization of cybermilitias through an otherwise ordinary technology company. They went on to say that at Nanhao, many of the 500 employees have a second job: since 2005, anyone under 30 has become part of the cybermilitia unit organized by the People's Liberation Army. It was argued that this operation is one of thousands set up by the Chinese military in technology companies and in universities.

In August, McAfee claimed to have uncovered Operation Shady RAT (remote access tool), a government-sponsored, cyber-espionage campaign that has been ongoing for five years against more than 70 public and private organizations in 14 countries. McAfee's VP of threat research said that these attacks were on an entirely different scale in that the targeted compromises are the work of an adversary motivated by a massive hunger for secrets.

The Economist, almost 1½ years ago, posited that after land, sea, air and space, warfare had entered the fifth domain: cyberspace. Examples dated back to the 2007 concerted denial of service attack on Estonian government, media, and bank web servers, which investigations traced to Russian 'hacktivists.' And similar attacks a year later during

Russia's war with Georgia, which appeared more ominous because they were coordinated with the advance of Russian military columns.

Just six days ago, Semantec issued a security response entitled, *Duqu, The precursor to the next Stuxnet*. The response was based on an alert they received on October 14th from the Laboratory of Cryptography and System Security at Budapest University. Duqu is described as essentially the precursor to a future Stuxnet-like attack.

Such are the dangers, but it is also true that in this same period of time, the Green Revolution occurred in Iran, and the Arab Spring uprisings were at least facilitated, if not fueled, in cyberspace.

Light and darkness; indeed, in the same season.

The world we now live in is hyper-connected, socially networked, and global. It includes another dimension that challenges our societal and organizational constructs, laws, and norms.

The means by which we address these challenges, from a technological and a policy perspective, has not yet evolved. Each new method of communication has brought such challenges as speed and scale grow.

With the radio, Sarnoff argued that the power of the network went as the number of people who had radios, N . With cell phones, Metcalf's law described the power of the network as N^2 , and today, Reed describes the power of the network using social media as 2^N . A connected, motivated group can now accomplish tasks otherwise thought impossible. At speeds and scales that we are only beginning to understand. It is one of the most intense challenges of our time.

The speed and scale of the network can be seen in examples such as the DARPA Red Balloon Challenge, where participants located 10 red weather balloons distributed in unknown locations throughout the United States in a startling 8 hours and 52 minutes. A task largely thought to be impossible using conventional methods. Or during the 5.9 magnitude earthquake that hit the east coast on August 23rd, when there were more than 40,000 tweets within minutes. And tweets from DC reached NY City ahead of the seismic wave itself.

Our responsibility is to acknowledge and prepare to protect the Nation in this new environment. We must recognize the interconnectedness of cyber as well as the duality of purpose it has revealed – peaceful instrument of global communications, economies, purpose, and productivity – and instrument for some, with other intentions, to threaten. We must both protect its peaceful, shared use as well as prepare for hostile cyber acts that threaten our military capabilitiesⁱⁱ.

The DARPA cyber analytical framework, which you will hear about later today, sought to quantify elements of the threat and create a context for understanding the question that we all face... Why? Why is it that despite billions of dollars in investment and the

concerted efforts of many dedicated individuals, it feels like we are losing ground? Through our analytical framework, we sought answers. We sought to understand why, so that we might build a stronger strategy.

This analysis, completed over months through original research and detailed investigation, concluded that the U.S. approach to cyber security is dominated by a strategy that layers security on to a uniform architecture. We do this to create tactical breathing space, but it is not convergent with an evolving threat. We discovered that we are losing ground because we are inherently divergent with the threat. Importantly, such divergences are the seeds of strategic surprise.

Let me give you one example: In response to the diversity and evolution of malware, cyber defense has moved from simple firewalls and application proxies to more complex firewall systems. The first appearance of “security appliances” shifted toward so-called unified threat management systems, which are now large and complex.

Over the last 20 years, using lines of code as a proxy and relative measure, the effort and cost of information security software has grown exponentially—from software packages with thousands of lines of code to packages with nearly 10 million lines of code. By contrast, over that same period, and across roughly 9,000 examples of viruses, worms, exploits and bots, our analysis revealed a nearly constant, average 125 lines of code for malware. 10 million lines of code versus 125 lines of code...

This is a striking illustration of why it is currently easier to play offense than defense in cyber, but importantly, it also causes us to rethink our approach. To seek new approaches that might lead to convergence. You’ll hear how later today.

This is not to suggest that we stop doing what we are doing now. On the contrary, our existing efforts are necessary. These efforts represent the wisdom of the moment. But if we continue only down the current path, we will not converge. Such persistence along the path would be foolhardy.

Wisdom and foolishness; indeed, appear in the same age.

Our objective today, is to open up a frank dialog about how we might change this situation. We believe we need more and better options. We will not prevail by throwing bodies or buildings at the challenges of cyberspace. Our assessment argues that in cyber, we are capability limited, both defensively and offensively. We need to fix it.

Our goal.

Our first goal must be to prevent war; we do so in part by being prepared for it. Failing prevention, however, we must accept our responsibility to be prepared to respond. We must do this while simultaneously acknowledging and protecting the basic freedoms of our citizens and with the protection of peaceful shared use of cyberspace.

DARPA's role, our initiatives, and investments.

DARPA's role in the creation of the internet means that we were party to the intense opportunities it created and share in the intense responsibility of protecting it.

I should emphasize that national policymakers, not DARPA, will determine how cyber capabilities will be employed to protect and defend the national security interests of the United States. But the Agency has a special responsibility to explore the outer bounds of such capabilities so that our nation is well prepared for future challenges.

To date, there has been much focus on increasing our defensive capabilities. To be sure, the list of capabilities needed is long. Our networks are safer than they were, but remain easily penetrated, passwords and accounts are hacked routinely, insider human or software threats compromise intellectual property and sensitive system information, the supply chain is not secure, and, because computers are embedded in all of our systems – cyber attack cannot be regarded a threat only to our networks and information – but rather to all our physical systems as well.

But, protecting cyberspace and the Nation will require both significantly enhanced defensive and offensive cyber capabilities. Capabilities across the full spectrum of conflict. And I mean technical capabilities. Modern warfare will demand the effective use of cyber, kinetic, and combined cyber and kinetic means.

Informed by these insights and with a willingness to accept our responsibility to contribute, we assessed that DARPA had a significant role to play; so, we recruited an expert cyber team made up of individuals from diverse experiences including the “white hat” hacker community, academia, labs and non-profits, major commercial companies, in addition to the Defense and intelligence communities. We launched several new initiatives; you will hear about many of them today. In summary, they are designed to change things. We need more options. We need more speed and scale.

Today you will hear about programs such as CRASH, which takes its inspiration from the defensive mechanisms of biological systems and seeks to develop cyber security technologies by radically rethinking basic hardware and system designs. And PROCEED is a big reach motivated by recent breakthroughs in fully homomorphic encryption, that could fundamentally change the nature of assured computations on untrusted hardware. Cyber Fast Track Initiative, which recognizes that an untapped pool of experts and innovators could contribute, if we provide a path. Because of time and security constraints, there are also programs you will not hear about, such as the Cyber Insider Threat program, or CINDER, which will develop capabilities for countering one of the most significant and malicious threats to military networks and systems: the cyber insider threat.

Since 2009, DARPA has been steadily increasing its cyber research. In our budget submission for FY12, we increased our cyber research funding by \$88M, from \$120M to \$208M. And over the next five years, our proposed investment in cyber research will grow steadily from 8% to 12% of top line. And we are also shifting our investments to

activities that promise more convergence with the threat and that recognize the unique needs of the Department of Defense. To this end, in the coming years, DARPA will focus an increasing portion of our cyber research on the investigation of offensive capabilities to address military-specific needs. We began these efforts on our own. But part of the growth in our resource commitment beginning in 2012 and extending through 2017, is at the hand of the senior leaders in the Department, who added \$500 million for cyber research at DARPA over five years.

DARPA's engagement in cyber is not new. This expanded effort rests on an existing foundation and continuing contributions to cyber. Indeed, DARPA-developed technologies are widely prevalent in both military and commercial use. But there is much to do.

DARPA activities are part of a larger whole within National Security at NSA, the newly formed CYBERCOMMAND, the Services, the private sector, universities, non-profits and as appropriate, DHS. Clearly, the challenges of cyberspace will require the concerted efforts of many. Indeed, to some extent, we all must be protectors of cyberspace.

But we should be clear; it will also demand the involvement of technical experts at unprecedented levels including in advisory roles during the formation of policy and legal frameworks, because new policies and laws (domestic and international) must be executable, enforceable, and sustainable.

To be of use, such policies and laws will demand evaluation and adjustment on time scales that correspond with the dynamic nature and compressed evolutionary timescales of advances in cyberspace. We'll have to move faster than we are accustomed. We'll need the tools and guidance to do so.

Cyberspace. Inhabited by humans.

More than forty years ago, the first packet-switched message was sent over the ARPANET. The first two letters of the word LOGIN were transmitted from UCLA to SRI before a buffer overflow crashed the system. Things have changed a lot in forty years.

Today the internet is commerce. It is a communal mind. It is both vulgar and sublime. Cyberspace is but a vast networked mirror that reflects the human race. In cyberspace, the best and the worst occupy the same time. Wisdom and foolishness are of the same age. Light and darkness are seasons. Joy is sorrow unmasked. Wherever we exist, inseparable, contrasting emotions exist, because otherwise, we feel nothing.

These are the timeless words of our existence.

It is true in cyberspace too.

ⁱ Charles Dickens, *A Tale of Two Cities*, 1859. Kahlil Gibran, *The Prophet*, 1923.

ⁱⁱ Excerpted from a speech by Former Deputy Secretary of Defense, Lynn.