

Cyber Noodle Soup no. 15

Welcome to the 21st Century. Don't make any sudden moves!

Ever heard of dimethocaine, methoxetamine or JWH-18? They are 'research chemicals' similar to cocaine, ketamine and cannabis respectively. They were all first synthesized in the last few years and are being produced in large quantities in Chinese factories. They are quasi-legal and readily available over the internet. As a consequence, they are already widely taken. Like mephedrone before them, it probably won't be long before they are banned. And, like mephedrone, no-one really knows if they are safe or not. People haven't been taking these new drugs for long enough for us to know. Scientific research is lagging far behind casual self-experimentation. Science can't keep up. In 2010, according to the European Monitoring Centre for Drugs and Drug Addiction, 40 completely new substances were taken by UK recreational drugs users. In the same year, 1,700 new medicines and drugs were licensed for the UK market. Many of these are psychoactive and some are liable to be abused. Psychopharmacologists and drugs professionals have a full-time job trying to keep up with the pace of change.

//

The XM25 is an airburst grenade launcher derived from the XM29 OICW. It fires 25 mm grenades that are set to explode in mid-air at or near the target. A laser rangefinder in the gun is used to determine the distance to the target. The user can manually adjust the detonating distance by up to three meters shorter or longer. The gun automatically transmits the detonating distance to the grenade in the firing chamber. The grenade tracks the distance it has traveled by the number of spiral rotations after it is fired. These features make the XM25 more effective than traditional grenade launchers at the task of hitting targets that are behind cover or dug into the ground.

//

The amount of business-related information processed by the world's computer servers in 2008 would fill enough books to create 20 stacks that would reach to Neptune and back, UC San Diego says in a study released on Wednesday. The unprecedented estimate says that 27 million servers distributed 9,570,000,000,000,000,000 bytes of data, or 9.57 zettabytes. A zettabyte is equal to a million gigabytes, or 10 to the 21st power. UCSD says in a statement, "The study estimated that enterprise server workloads are doubling about every two years, which means that by 2024 the world's enterprise servers will annually process the digital equivalent of a stack of books extending more than 4.37 light-years to Alpha Centauri, our closest neighboring star system in the Milky Way galaxy. Each book is assumed to be 4.8 centimeters thick and contain 2.5 megabytes of information."

//

As the economy continues to improve, demand for facelifts and other facial rejuvenation surgery will increase. Non-surgical facial rejuvenation procedures will also see some growth, but people who have been putting off surgery for the past few years because of the economy will be ready for the gold standard in facial rejuvenation in 2011.

The growth and popularity of cosmetic injectables (Botox, Dysport, Sculptra, Radiesse, Evolence, Juvederm, Restylane, Perlane etc.) will continue to increase as products continue to evolve and new players enter the market.

Consumers looking for a bargain on cosmetic procedures will unfortunately lead to an increase in horror stories about "discount injectables" bought offshore and cosmetic medicine and cosmetic surgical procedures performed by untrained or poorly trained practitioners.

In the coming year patients will be seeking posterior body lifts, buttock lifts, surgical and nonsurgical buttock augmentations to shape and augment their buttocks.

//

Cyber-crime cost a staggering US\$114 billion in the last year and claimed 431 million victims, according to security company Symantec. Cyber-attacks cost the United States \$32 billion in direct financial losses, China around \$25 billion, Brazil \$15 billion and India \$4 billion, the Symantec's 2011 Norton Cybercrime Report claims.

Over two-thirds of Internet users have been victims of cyber-crime at some stage, which totals more than a million victims per day; 85% of respondents to the Norton survey, carried out in 24 countries with 20,000 people, claimed they had been victims of a digital scourge that is rapidly spreading to mobile phones.

The report said men between the ages of 18 and 31 who access the Internet from their mobile phones are most likely to be targeted; 80% in the group reported being the victim of a mobile cyber-crime.

Social networking websites were also cited as being prime hunting grounds for scammers and digital criminals who can easily prey on a click-happy contingent of users. A disconnect with the threat was also evident as 74% of those surveyed stated that they were aware of cyber-crime but failed to take any precautions to prevent it.

//

This very moment, grazing in the fields of the State Key Laboratory of Agrobiotechnology in Beijing, China is a particular herd of about 300 cows. Each one is a clone, and each one produces milk that contains proteins normally found in human milk. The cows are part of a vision belonging to Ning Li, SKYLAB's director, to put "human-like milk" onto supermarket shelves—and into baby bottles—all over the world.

As published in the Public Library of Science One, the cows were cloned by somatic cell nuclear transfer—the same method Ian Wilmut used to clone Dolly—in which the nucleus of a somatic (body) cell is transferred into an egg that has had its nucleus removed. Prior to inserting the somatic nucleus into the enucleated egg, Dr. Li's group infected it with a virus carrying the human gene for lysozyme. Lysozyme is an enzyme found in large quantities in human breast milk that can lyse—or split open—the cell walls of harmful bacteria in the gut. In addition to its antibacterial effects, lysozyme works to boost the body's immune response to infection. The immunological benefits imparted by lysozyme is an important reason why breast milk is so healthy for developing babies. It's absent in most of the baby formulas commonly-used to supplement or substitute breast milk. Compared with the 200-400 µg/ml concentration found in human breast milk, cow milk normally contains lysozyme at 0.05-0.22 µg/ml. The milk from Dr. Li's cows increased their lysozyme concentrations more than a hundred-fold to 26 µg/ml.

//

Labor camp workers in northeast China are being forced to play online games in a money making scheme for the guards. Up to 300 workers at the Jixi labor camp in Heilongjiang province have been found "gold farming", a practice that involves collecting online credit in games such as World of Warcraft. The credit, which is usually accrued by completing repetitive menial tasks in the game, can then be exchanged for real money with other players.

The practice, which is technically illegal, is widespread. Players in developing countries often accumulate vast amounts of gaming gold that can then be sold to those in Europe or the US. In an interview with The Guardian, prisoners spoke of 12 hour shifts and punishment for not completing their digital work quotas. Guards had been rumored to be earning 5-6,000 yuan a day (US\$770-\$920) from the scheme.

Officials representing labor camps in China denied the claims. Gold farming is big business in the People's Republic; an estimated \$2 billion in online gaming currencies was traded in 2008, and roughly 80%

of all the gold farming in the world is done in China, where more than 100,000 people make a full-time living from it.

//

Millions of Americans have implantable medical devices, from pacemakers and defibrillators to brain stimulators and drug pumps; worldwide, 300,000 more people receive them every year. Most such devices have wireless connections, so that doctors can monitor patients' vital signs or revise treatment programs. But recent research has shown that this leaves the devices vulnerable to attack: In the worst-case scenario, an attacker could kill a victim by instructing an implantable device to deliver lethal doses of medication or electricity.

Today's implantable medical devices weren't built with hostile attacks in mind, so they don't have built-in encryption. But even in the future, says Dina Katabi, an associate professor in MIT's Department of Electrical Engineering and Computer Science, handling encryption externally could still prove more practical than building it directly into implants. "It's hard to put [encryption] on these devices," Katabi says. "There are many of these devices that are really small, so for power reasons, for form-factor reasons, it might not make sense to put the [encryption] on them."

//

Its name is TDL-4, and they say it's invulnerable. Known as a botnet, this malicious software has infiltrated an estimated 4.5 million PCs around the world, using them without their owner's knowledge and turning them into the silicon equivalent of zombies. There are many active botnets, and many more have been defeated by anti-virus security firms, but TDL-4 is special – it's advanced. This cutting edge botnet can remove competing malware, install malware of its own, and rent out its network for spamming or phishing ventures. It communicates on multiple channels, with millions of infected computers receiving commands over public peer to peer (P2P) networks. TDL-4 even buries itself in the master boot record, making it invisible to your operating system and security software. In short, TDL-4 is one of the most sophisticated pieces of malicious software that has ever been put forth on a global scale, and it's just getting warmed up.

//

Unlike bombs, missiles, and guns, cyber weapons can be copied. The proliferation of cyber weapons cannot be controlled. Stuxnet-inspired weapons and weapon technology will soon be in the hands of rogue nation states, terrorists, organized crime, and legions of leisure hackers, some of whom are just waiting for a better thrill than World of Warcraft. This is a very distinctive difference to conventional (hardware) weapons. Even if it is known, for example, how nuclear weapons are built, not everybody who wants to possess them is capable of developing or even acquiring such weapons. For cyber weapons, this will be different. Cyber weapons can and will be copied, reused, and will be available for cheap money on the Internet. At some point in time, they will even be available as freeware.

Such Stuxnet-inspired weapons will soon look different from the original. Stuxnet was precisely designed for surgical attacks on distinct targets. It is obvious from code analysis that the attackers had access to internal product and installation details, and the engineering talent to turn such technological insight into sophisticatedly engineered attacks. There is absolutely no reason to assume that follow-up attackers will follow the same philosophy. Just to the contrary, other attackers will most likely not invest the engineering effort for similar pinpoint attacks. It is much more likely that we are going to see "dirty" digital bombs in the wake of Stuxnet, meaning bombs that hit without nearly the precision as we see it in Stuxnet. The real concerning threat of cyber weapons is not a surgical military strike as we have just seen it with Stuxnet, it is the dirty digital bomb. The dirty digital bomb is a cyber weapon that inflicts low to medium damage to a large number of random targets. It doesn't require experts. Any idiot can assemble and use it. And while the individual damage that such dirty digital bombs can cause may not nearly be as big as in Stuxnet's case, what makes

them even more dangerous is the fact that small damage in many power plants may be worse than big damage in one specific power plant; small damage at many automotive suppliers may be worse than big damage at one specific car maker.

//