Design has a history of violence, yet professional discourse around design has been dominated by voices that only trumpet its commercial and aesthetic successes. Violence, defined here as the manifestation of the power to alter circumstances against the will of others and to their detriment, has always been ubiquitous, and in recent years technology has introduced dramatic new threats. Design and Violence sheds light on the complex impact of design on the built environment and on everyday life, as well as on the forms of violence in contemporary society.

Published to accompany an online experiment launched by The Museum of Modern Art in 2013, this book brings together controversial, provocative, and compelling design projects with leading voices from the fields of art and design, science, law, criminal justice, ethics, finance, journalism, and social justice. Each author responds to one object—ranging from an AK-47 to a Euthanasia Rollercoaster, from plastic handcuffs to the Stuxnet digital virus—sparkling dialogue, reflection, and debate. These experimental and wide-ranging conversations make Design and Violence an invaluable resource for lively discussions and classroom curricula.
Patrick Clair’s motion infographic Stuxnet: Anatomy of a Computer Virus thoughtfully animates the inner workings of the elusive malware Stuxnet. This intricately constructed computer virus, consisting of a worm, a file shortcut, and a rootkit, was designed to disrupt programmable logic controllers, or PLCs, run on Microsoft Windows operating systems. PLCs typically control automated manufacturing and monitoring processes, such as industrial-plant assembly lines. The Stuxnet virus works in two waves: first, it maps a blueprint of the plant operating systems; second, it disrupts these systems. By exploiting unknown security gaps, the virus was able to destroy twenty percent of Iran’s nuclear centrifuges, while simultaneously relaying normal readings to the plant operators. The attack was delivered via USB thumb drive, and although it was first detected in June 2010, it may have been circulating for up to a year prior. The malware, which has been linked to a policy of covert warfare allying the United States and Israel against Iran’s nuclear armament, is considered to be the world’s first weaponized piece of software and heralds a change in twenty-first-century global military strategy. Its creators remain unidentified.
MoMA DESIGN & VIOLENCE
Paola Antonelli and Jamer Hunt

Stuxnet: Anatomy of a Computer Virus (Patrick Clair, 2011)
Lev Manovich

My own first encounter with design and violence was at the age of 15. As a high school student in Moscow, I had to take two years of mandatory classes in military education. Over many months, we practicing disassembling and reassembling the masterpiece of the "design meets violence" genre: the legendary Kalashnikov rifle. Because it consists of only a handful of pieces, I was able to disassemble it in eleven seconds, and put it back together in sixteen. (Dismantling the rifle within a certain time was required for passing the course).

I suppose this background gives me some qualification to reflect on projects in the Design and Violence initiative, such as Patrick Clair's video infographic on Stuxnet, a computer worm unleashed on Iran's nuclear program, amongst other target sites, and discovered in June 2010. Computer worms, as with viruses and executable scripts, constitute part of the various tools and techniques in the arsenal of cyberwarfare and cyberspying. If mid-twentieth-century non-networked weapons such as the Kalashnikov are location specific, operating only within their user's immediate line of sight, viruses and worms are not hampered by geography: worms such as Stuxnet can replicate and move from computer to computer around the world, attacking not only the host system but also its hardware and the other computers it controls.

Stuxnet is the first known computer worm to spy on and reprogram industrial systems. It indiscriminately hops across computers that run Windows-based operating systems, but its malware specifically targets industrial software from Siemens that is used to control a variety of large-scale infrastructure systems, including manufacturing plants. Stuxnet affected facilities in a number of countries, including Iran, Indonesia, India, and the United States. Due to its size, and the unusual complexity of its code, it has been speculated that the worm was developed by a nation-state. (According to a 2012 New York Times op-ed, the United States and Israel collaborated on its design.1)

Because Stuxnet has been in and out of the news for a few years now, there are a number of well-designed media presentations explaining its history, effects, and operations (besides dozens of articles). They include a compelling diagram by Guilbert Gates that accompanied a New York Times op-ed,2 and a dynamic 2011 TED video from the German scientist Ralph Langner, who worked on an analysis of the worm.3 (At the time of writing, the video had received over one million views.) As always, the most detailed single source is the Wikipedia page, which, as of December 2014, has been edited 1,529 times by 716 distinct authors, and has received over 62,035 views in the last thirty days alone.

Knowing about all this coverage of the Stuxnet worm helps in thinking about Patrick Clair's video, produced for an Australian TV program in 2012. In contrast to the more complete historical narrative presented on Wikipedia, Clair's video presents only one of its dramatic episodes: the discovery that Stuxnet affected Iranian nuclear reactors. The video uses the contemporary language of motion graphics, with animated 2-D and 3-D text, unexpected 90-degree camera turns, superfast zooms, and 3-D vector graphics. As is typical of such videos, the movement never stops; forms are transposed, transfigured, added, and multiplied without pause. This constant movement is visually engaging but also troubling. The constantly flowing animation works differently than broadcast-news segments that typically cut between the newscaster's narration, live and recorded interviews, and on-the-scene reporting. These cuts or breaks may interrupt...
the viewer’s immersion in the story, but they also leave space for the viewer to digest and better understand the information presented. In the motion-graphics narrative, however, there are no such breaks or juxtapositions of media types; instead the story unfolds in one continuous three-minute-long animation accompanied by a constant music beat in the background. The color wireframes and robotic-camera moves look cool, but all too often at the expense of the important facts and details of the events being described.

Branding Stuxnet as “the first weapon made entirely out of code” (this may be true or not, depending on your definition), the video tries to convey the worm’s operation through visual forms and metaphors. For example, at 1 minute 30 seconds, the familiar Kalashnikov rifle appears on the screen, presented as a wireframe model. The rifle multiplies and shrinks to spell the word “code,” linking the physical and electronic forms of assault weaponry. (It reminds me of how, at the end of our course in my Moscow high school, we were taken to a real military range out of town to practice what we learned. My fellow students and I, each with a heavy Kalashnikov in hand, lined up across a white winter field and then shot at the targets.)

Projects such as Clair’s exist within a paradigm I call “info-aesthetics.” These projects, which arise not only from the field of data visualization but also from motion graphics, human-computer interaction (HCI), architecture, music and custom hardware, to name a few, have as their true subject the “stuff” our software society is made from—data (big and small), algorithms, distributed client-server systems, global networks, networked hardware. And, as with these other works, Clair’s video tries to give this stuff a visible form in order to make sense of it and to produce knowledge from it. But because data and code largely exist at a scale outside of that of the human body and perception—because they are too big, or too fast, or too dispersed—the task is quite hard.

Which leaves me with the same questions I’ve been asking for years: Can our information society be represented iconically, if all its most characteristic activities are dynamic processes? How can the superhuman scale of our information structures be translated to the scale of human perception and cognition? Clair’s video dramatizes how challenging a task this is for contemporary designers. Were we to remove the video’s familiar objects—the microscope, the schematic diagram of a nuclear plant, the rifles, and the text, what would be left? Is it possible to visually represent a software “thing”—in this case, Stuxnet—that operates on a scale radically different from the old, familiar Kalashnikov rifle?

Lee Manovich is the author of three books, including The Language of New Media (Cambridge, Mass.: The MIT Press, 2001), and a professor at The Graduate Center, CUNY.

THANK YOU