A Look at Anonymous and Anons During its #OpIran Mission, February 14th-18th

Basic rule: Blend in with the crowd, disperse into the stream. Keep a low profile. Don't try to be special. Remember, when in Rome, do as Romans do. Don't try to be a smart ass. FEDs are many, Anonymous is Legion, but you are only one. There are no old heros, there are only young heros and dead heros."
Anonymous-the uber-secret handbook, compiled by Anonymii, version 0.1.3, date 15.02.11

Anonymous: amorphous, a title for the un-named; you can't pin it down, and that is very much the point. Yet its law-skirting existence depends upon an unceasingly expanding list of highly specific instructions and directives, and an intrinsically motivated sense of Justice. The Wikipedia entry for Anonymous (which I assume Anonymous finds satisfactory or else it would have long ago been modified) defines it as a meme “representing the concept of many on-line community users simultaneously existing as an anarchic, digitized global brain”. Representation of a Concept via Meme...assuming this mind-breaking characterization was deliberately constructed by its Wikipedia author, perhaps it captures just what makes Anonymous one of the most compelling and mis-categorized phenomena in digital current events.

Anonymous maintains a unique form of self-definition by creating and underlining a split between its self-conception and the execution of its self-driven goals. In effect, it splits itself off from either concept or execution, and then functions as the invisible, tacit string holding them together. The execution of concept is carried out by those sufficiently aligned with the idea to fly the Anonymous flag; to be Anons. This complicated structure allows for constant revision of both the concept of Anonymous and the execution of its operations, while keeping the greater meme intact.

Anonymous is found nowhere specifically at any given point of time, until those flying its flag coalesce at certain points to engage in highly specialized disruptive acts directed towards constantly shifting targets. Its structure is as transparent at the macro level as it is opaque at the micro level. The transparency facilitates many observers, but it is the obfuscation of its individual members, via continually modified tech-dependent procedures, that makes it possible for it to operate at all.

Anonymous' iterative self-realization goes hand in hand with the inherent instability of its structure. Just as a wall only keeps out invaders for a certain period of time and necessitates an ever-changing defense system, “Security is a continuing process, not a state”. All discussion and structure is treated in such a way that responsibility rests entirely with those who carry the flag; thus they are advised to conduct “regular audits and encrypted backups”. Security for Anons is security for Anonymous. It would be ridiculous and impossible to go after a meme, but a lazy Anon can end up on an FBI investigation list, and indeed, that is what happened to a number of Anons in December 2010.

In Anonymous-the Uber-Secret Handbook, compiled by Anonymii, version 0.1.3, date 15.02.11, Anonimii state that “The greatest threats to your safety are A) social engineering and your behavior and

1 http://en.wikipedia.org/wiki/Anonymous_%28group%29
2Anonymous-the Uber-Secret Handbook, compiled by Anonymii, version 0.1.3, date 15.02.11
B) revealing your IP address.” You are instructed to “not give any personal information on the IRC chat as it is public, you mom could read what you write there and so could the Police. And don't mention your involvement with Anonymous in your real life.” The handbook lays out at a micro level a specific list of procedures designed to prevent the unmasking of Anons.

Among Anonymous' recent best known acts are DDOS attacks on Amazon, PayPal, MasterCard, Visa, and recently the HBGary website (also hacking into company email, uncovering a decompiled version of Stuxnet, the code of which was uploaded to Github and posted to Twitter on February 19th). DDoS attacks are conducted via “Hive Mind”, in which participating Anons voluntarily activate a program called LOIC on their computers, to form a voluntary botnet.

Though there is no center or single central meeting point for Anonymous, there are stable and temporary nodes into which both participants and observers can enter. The AnonOps forum at http://www.anonops.net/ has permanence. My entry into Anonymous came via AnonOps.net, which considers itself an Ops meeting node, made viable through “free speech hosting” via provider Heihachi.net, “DDos Protected Offshore Bullet Proof Hosting” “here to provide a service for anyone to speak freely on a subject”.

AnonOps.net emerged from pro-Wikileaks Operation:Payback as a security solution for operations conducted by Anonymous, yet it forcefully outlines its organizational autonomy: “We are not Anonymous. We are not 4chan. We are not Operation: Payback and we did not attack any websites. We are merely a network frequented by their movement”. I spent time on AnonOps.net long enough to find Internet Relay Chats of interest, but from that point on I would directly enter into the IRC via URL link.

Internet Relay Chats are where Anons engage in real-time communication; setting directives, comparing notes, and shooting the breeze. The most vital characteristic of the IRCs is that there is no facility or mechanism to archive conversations. A user can enter the IRC either through a server port or link. Using a server port, in conjunction with VPN software, allows for greater security by masking your IP. During my investigation, I did not download the chat client needed to connect through a server port, perhaps compromising my own security (though I did not participate in any missions via LOIC or in any other respect).

New IRCs form as chat participants, Admins, and Operators identify situations ripe for intervention, thus the IRCs become devoted to special “Ops” and topics. Suggestions from Anons are considered by the Admins and Operators. Channels fluctuate in participant numbers and facilitate large conversational breadth, which can cover at any one time both technical updates and asides into “( o ) ( o )” and “8====D”, though this type of 4chan-style sharing tends to be met with reprimands to get back to the Current Channel Topic.

While anyone can theoretically become involved in the Ops, one must be sufficiently motivated to find information for entrance into discussion forums and real-time conversations. Those who participate in Ops by following specifically laid-out instructions experience a satisfying direct line from their pooled actions to outcomes. An Anon feels a swell of pride at the successful defacement of a website, knowing that it was their vital link, (via LOIC) into the voluntary botnet that made it possible. By defacing a website, Anons make a statement that propagates their message and hopefully inspires activists native to the situations they have taken up cause with.

It seems pride is also fed by feeling at some level that Anons are actual soldiers with real firepower.
The term “Low Orbital Ion Cannon” is a joke, but the language around using it is humorously jingoistic:

[14:44] <Guieth> I'M FIRING MAH LAZER!
[14:44] <@nimbus> FIRE
[14:44] <n0n3unkn0wn> BOOM

Sense of belonging seems both driven by a desire to share a certain brand of humor and to generate results that give it form. For Anons, humor is political.

[12:24] <&efg> godbert: among our ranks we have quite a number of those that do it for the lulz”
[12:24] <mao> anonymous is powered by the lulz”.

What came next showed an inherent self-consciousness about the historically schadenfreude-tinted sensibilities of Anonymous, and its 4Chan origins:

[12:24] <&efg> revsol: I don't think it necessitates giving up. I like tilting at windmills. But I have no illusions about people being intrinsically good and kind”.
[12:25] <+muninn> <revsol@I2P> efg: Fine. Lets take that. There is no intrinsic need for goodness. Superficial goodness will do.-
[12:25] <+muninn> <revsol@I2P> Convenience will do.-
[12:25] <+muninn> <revsol@I2P> Fear will do.-
[12:25] <+muninn> <revsol@I2P> (AND some, some just some, might be good, or good enough, or temporarily good enough...
[12:25] <godbert> haha regardless efg, even if its not for the cause of "good" the good is getting done”.

Desire for “Lulz” certainly motivates Anon missions, but one might go so far as to say that Lulz becomes a political quest for justice rather than a desire to punish primarily for hilarity's sake.

On February 14th, in parallel with the fledgling protests on the ground, AnonOps created a new channel, #OpIran, in which discussion and strategy building began for how best to assist protestors and dissidents on the ground. CommanderX, identifiable as either the channel Admin or Operator, quickly put forth a downloadable “care package” for a “White Fax Spam Campaign” utilizing free internet fax. The package contained general notes of encouragement, as well as instructions for Iranians to create secure internet connections via use of I2P, which “will act as a relay and make the network more robust for the Iranians”. (Previously Anons used TOR, but “Iranian security services are blocking access to TOR somehow”). Concurrently, #OpIran began a series DDoS attacks against leader.ir, basij.ir, justice.ir, mfa.gov.ir:

[18:39] <@CommanderX> This is an ALL NEW White Fax/Spam campaign focusing on I2P which we have packaged into a nice little 10 mb download we are calling Op Iran Care Package Light. it contains I2P, a cool Op Iran poster/flyer and the Farsi instructions on the LOIC. The URL for this new action is the same as the last, I simply updated the page with the new info - so if you already have the old one bookmarked just refresh and you go it. So, it's here.

After CommanderX's initial instructions, Chuck took up the torch, reiterating the Channel Topic every few minutes for new IRC entrants, and modifying it nearly hourly in accordance with changing instructions:
On February 14th, Anons in the IRCs were riding high after success with #OpTunisia and #OpEgypt, their contributions falling within the more meaningful, effective noise social media had arguably managed to create. #OpTunisia was seen to have successfully inspired Tunisians to conduct their own “hacktivism”. Of course, there is a meaningful distinction between AnonOps' unique brand of “hacktivism” and forms of expression made manifest via other social media platforms. While the act of tweeting is facilitated, publicly sanctioned, and designed to minimize barriers for new users, hacking, when unsanctioned, can be a disruptive, self-initiated activity that pushes the actor outside the spheres of law; accountable only to oneself, yet bound to very specific, iteratively built protocol. To hack requires both an anti-establishment mindset and a dedication to a very specific sequence of actions that require high skill and follow-through.

In the case of Anon's involvement in the Middle Eastern protests since December 25th, the act of defacing an official government website is intended to both propagate Anonymous' message to the media, and to inspire activists native to the situations AnonOps has taken up cause with to propagate anti-gov actions into both virtual and “meat space”. By the evening of February 14th, #OpIran had managed for intermittent periods to take down Leader.ir, khamenei.ir, http://parliran.ir, and president.ir. This begs to question how one qualifies a Op to be a success. Does only intermittent website downtime signify failure? The #OpIran metrics for success entails assorted Op members checking the DDoS'd site to see if it is accessible, excitedly pointing out if it appears to be down, and then checking in for confirmations from others:

[12:30] @gc7! check irna.ir
[12:30] @evilworks gc7: It's not just you! http://irna.ir looks down from here.
[12:32] @nimbus if we can get to them - long shot but low cost - it would do much good.
[12:34] @muninn <revsol@I2P> (Likes "low cost / good result" ratio way of puttin' things. That is, partially, it.) ;)

From February 14th-19th, @evilworks appeared to consistently to spearhead the QA; for all 5 days that I followed the chat, he remained in charge of confirming successful DDoS attacks. In these missions, success is often not something achieved instantaneously or decidedly. It's understood that success is tenuous, but this is accepted as it comes at “low cost”. Later in the day, Ops member +bishop gave an international rundown which @evilworks confirmed. This lead to an outpouring of encouragement among Ops members:

[15:39] @bishop Good work, Gentlemen.
[15:39] @efg nicely done, that was quick
[15:39] @efg now keep it down :D
[15:40] @sh4ri4 good work
[15:40] @nimbus hoho lovely
[15:40] Whitey gogogo
[15:40] chaos_rorschak good work
* sh4ri4 is proud of the little channel that could

Though specific defacements are pursued for extended periods of time, members participate in an organizational feedback loop, providing new suggestions when certain targets seem unrealistic:

[12:39] <WebAnon2231> FORget irna.ir
[12:39] <WebAnon2231> go for bmi.ir
[15:23] <&efg> hey chaps, the target's changing again soon
[15:25] <&efg> :D
[15:25] <&efg> thank you for waiting, though!
[15:25] <@nimbus> Target's changed, people :)

From Monday 2/14 through Tuesday 2/15, the amount of chat users in the #OpIran IRC increased about three-fold. Some were carry-over from previously active channels (#OpEgypt became very quiet), but a number of users of the IRC were newly interested observers made aware of AnonOps via mainstream media. IRC coordinators periodically offered to PM (private message) with any journalists in the IRC, and I saw responses to this solicitation twice on 2/15. There seemed to be a direct line in place between action coordinated via IRC, and media coverage; it took no longer than a few hours of substantial activity in the channel for the wall street journal to make note of OpIran.

“[20:20] <TarenCapel> hey we're in the Wall Street Journal guise”.

At 4:31, on the same day that the OpIran IRC channel was created, Cassel Bryan-Low wrote for WSJ.com that “the online collective known as "Anonymous," which has attacked a number of corporate and other websites in apparent retaliation for moves against the document-leaking organization WikiLeaks, said Monday it has turned its attention to Iran.”

On Wednesday 2/16, I was surprised to see that I could no longer automatically log into the #OpIran IRC. In a surge of panic, I logged into #OpEgypt, still open but quiet, asking “hey guys, do you know what's happening with the #OPIran IRC? I can't log in”. Within 10 seconds I received a reply from a IRC member ; “I will check”. After another 10 seconds, I received access as a newly registered user to the #OpIran IRC. This seemed to show an almost instantaneous pace of coordination among the Operators and Admins of the IRCs. This also seemed to mark a point at which Ops members had decided that consolidation and security were more important than recruitment and outside observation.

The increased security of the IRC coincided with the point at which it became clear that Iranian protests would reach no tipping point.

[12:29] <@gc7> guys the protests in tehran were very crowded but disperesed, hearing back from lots of people at home
[12:36] <+Effexor> Derp! Iran protest crackdown condemned | Amnesty International
[12:30] <Slavenomore> iran will not be as egypt
[12:40] <+Effexor> Derp! BBC News - Iran police fire tear gas at opposition rally in Tehran
[12:41] <mib> reports of Iranian republican guard on the streets
[12:41] <WebAnon2231> lol
[12:41] <WebAnon2231> sure?
[12:41] <mib> this is getting serious
[12:42] <@proSI> wow, protests in portugal are planned for March 12... this is the year of protests!
Aside from on-topic conversation, the “quality” of the conversation in the #OpIran IRC was variable. Most conversation seemed inoffensive and cordial while the group remained on task, but interjections came with fair frequency:

“[12:08] <AnonCat> Fuck the Jews, no offence (sic)”. 

This came on day 4 of the Op, on 2/17, at which point morale was low. Discussion turned to a general indictment of colonialism. One user took pains to point out a genocide of “500k jews by Hitler” had lead up to the founding of the Jewish state. It was at this point that I felt compelled to interject for the first time, typing simply “FYI 6 million”, to which the Anon cordially typed back; “noted, 6 million”. Such a knowledge gap felt surprising and disorienting, and yet somehow fits with the unfiltered multitude of backgrounds in the unhedged membership of the IRCs. At least the Anon was cordial in response to a (personally-motivated) interjection by a “No0b”.

During the 5 days spent in the #OpIran IRC, there was one major point of contention between Anons. While the Anonymous handbook lays out definitely that Anons should never attack media, on February 17th, #OpIran leads decided to pursue the Islamic Republic News Agency, Irna.ir.

As the debate kicked, up, Chuck changed the official topic of the channel to reflect what was obviously an argument of a certain significance. 11 minutes later, the debate was closed, and the Current Target became Irna.ir.

The controversy of attacking IRNA seemed to get the ball rolling on discussion of carrying out further controversial acts. Ultimately, IRNA seemed to be as far as anyone was willing to cross the line in the period that I observed the IRC.

The controversy of attacking IRNA seemed to get the ball rolling on discussion of carrying out further controversial acts. Ultimately, IRNA seemed to be as far as anyone was willing to cross the line in the period that I observed the IRC.
This exchange demonstrated that while conversation is free and suggestions are taken, potential acts are debated in the context of the greater moral code of Anonymous. When the code, as laid out in Rules of Anonymous, is intentionally breached, it is done soberly and with exception.

After observing such a uniquely calibrated system of operation, it is difficult to determine what would make a beneficial design change for Anonymous, AnonOps.net, or the IRCs. The breach of the Rules of Anonymous in the service of attacking government run media website IRNA seems like a big deal for group dynamics; opening the door to further contention and possibly poisoning the pure Liberty/Justice-seeking code “Anonymii” promote in the IRCs and handbook:

(excerpt from Anonymous-the Uber-Secret Handbook):

Q: Why not attack that newspaper/TV/Radiostation?
A: Anonymous does not attack media.
Q: That is no media! It only spreads lies and propaganda!
A: Freedom of speech counts for assholes too³

Though it is probable that their attack on IRNA is what caused a temporary DDoS attack on their servers on 2/16, a DDoS attack in retaliation of Anonymous seems almost inevitable, and #OpIran took it in stride.

What initially drew me to look at Anonymous was the news on January 29th that the FBI issued 40 search warrants in connection with various DDoS attacks carried out over the past year. The FBI's tactics seem to be more sophisticated than those undertaken by HBGary's CEO, who claimed he'd identified all key leaders of Anonymous through a unique means worthy of Government investment: drawing lines between login times on Twitter, Facebook, and IRCs and the content posted to respective accounts. What's funny is that his means are either directly inspired by the Anonymous handbook, or directly lead Anonymii to update their security advice within the Handbook. Which came first?

Excerpt:

* Never connect at same time. Try to alternate.
* Do not post on the public net while you are in the IRC, and definitely do not mention that you are posting something on Twitter. This is easy to correlate.
* Don't discuss whether you personally are DDOSing or writing How-Tos or Nmap'ing the target, making graphics etc. or not, just discuss general strategy
* Do not post pictures hosted on Facebook. The filename contains your profile ID.
* Stagger your login & log out times on FaceBook, Twitter & IRC. They can be compared for user info.

³Anonymous-the Uber-Secret Handbook, compiled by Anonymii, version 0.1.3, date 15.02.11
I would conclude that the design of various operations undertaken by Anonymii revolves around a shifting tradeoff between security and goal-seeking, and that Anonymii act immediately to address inadequacies in security as they arise. The next “design” decision will be made when the walls have been felt to be breached. In the meantime, Anons must negotiate the ramifications of the exceptions they make to their own rules.