The bizarre online hubs and the role they play in the online information and culture wars, by Greg Rowett of the Institute of Statecraft

"If your opponent is of choleric temper, seek to irritate him" â€“ Sun Tzu.

Information warfare is not the flashiest, most glamorous, form of war. This paper was originally a briefing to the U K Defence Forum, aiming to cover the fundamental concept and highlight some of the key challenges faced by the West in responding to infowar, and how information warfare has evolved in recent decades.Ã‚Ã‚Â It's a perfect storm, and quite possibly, an existential threat to democracy.

The concept of information warfare is as old as war, and references to it in one form or another can be found in almost every major text on strategy, though rarely using the same or similar terminology. It is elusive, and straddles an area between military and domestic strategy that has often proved problematic for those with a mind to the separation of domestic civilian issues and military matters, a lapse that could be excused for most of history, though no longer. However, it is relatively straightforward. It is the use of information as a tool to impose ones will upon the enemy â€“ in the same manner that any other tool of power is used in war. My preferred definition, based on the US Navy definition of psychological operations is:
'The organised and deliberate use of communications, information and psychological operations to influence or disrupt the emotions, motives, objective reasoning, decision-making abilities and ultimately the behaviour of foreign governments, organizations, groups, and individuals in pursuit of a strategic advantage.'

Which is wordy, but effective. In essence, in all war â€“ particularly wars involving the citizen soldier and the mobilisation of society â€“ the main objective is to overcome the enemies will to resist. All physical goals are about bringing about that reality. This can be done by physical means â€“ i.e. defeating their army in the field and forcing them to pragmatically concede the point of contention â€“ or more indirectly - undermining or overwhelming the foes economy to the point that they cannot sustain their opposition. But without breaking the enemies will to fight, they may continue to do so far beyond what one might expect to be reasonable, even unto their total destruction, or â€“ occasionally â€“ their triumph if they outlast your own will to fight. Emperor Napoleon: "In war, moral factors account for three quarters of the whole; relative material strength accounts for only one quarter."

Perhaps the most recent and notorious example is the US's Vietnam war, where on practical terms the US had the material means to fight at their current rate of attrition almost indefinitely, whilst suffering far fewer casualties â€“ both in direct numbers and also as a proportion of their population â€“ than the Vietnamese. Yet the US was not able to sustain its will to fight, with its population becoming opposed to the war and sapping its political leaders of the will and ability to continue. Information warfare, is about using information, rather than other means, to attack that will to resist.

So information warfare has existed, in some form or another, for as long as war itself has. Its form has changed of course â€“ moving from grand displays of power and divine favour in antiquity, to the dissemination of propaganda leaflets from planes, and radio in more recent times. But the biggest and most revolutionary changes â€“ greater than the printing press, mass media, total war, and nationalism â€“ has been the internet, and social media.

Social media is not just Facebook, Twitter, and so on. The social media system â€“ and when I refer to social media, I refer almost exclusively to the online form â€“ far outdates those platforms. It has innumerable forms - the earliest social media sites were simple chat rooms, where people gathered online and interacted. Most of these communities had no barrier to entry, and were anonymous. Indeed, while most social media platforms these days endeavour to draw out as much personal and private information as possible, these earlier forums were almost entirely anonymous, with communities that were simultaneously welcoming, and fiercely hostile to 'outsiders'.

This sentiment remained, and as the internet developed and its usage exploded, one of the demographics that was at the centre of these communities were gamers and weebs â€“ weebs being a term for fans of anime and Japanese media. Gaming and anime are perhaps not the subjects that you would expect to see in a piece on infowar, but given the impact that their communities have had on the development of online culture, they must and should be included. Both these interests were not seen as 'cool' for a long while, and even now their communities often feature a lot of defensive counter-culture. The stereotype of a social outcast â€“ mostly young males â€“ can fairly be said to be true. These communities however, were and remain some of the most influential groups in terms of content production on the internet. The memes, jokes, and other 'e-culture' quirks produced in these smaller communities are exported around the internet, carrying the cultural impressions embedded within that content. One example is Pepe the Frog, a green cartoon frog which achieved fame in the 2016 US election cycle that has become associated with the so-called 'alt-right'.

But before that, these communities were relatively politically benign, instead mostly focusing around whatever special interest linked them together. Meme wars and minor friction existed between these communities and others â€“ most notably the emerging 'social justice warrior'

(SJW) internet subculture, which could be described as the 'alt-left'. Both sides saw the signs of the other everywhere, seeking to impose their agenda upon them. These communities form what could be called the 'grey web' â€“ riding a line between the mainstream sites frequented by most people online, and flirting with the darker and more sinister aspects of the internet. The content and focus of these communities is not illegal, but they tend to pride themselves on being a level below the safe experience of most internet users, and often boast smaller but incredibly active userbases. They have an air of mystery and danger to them which simultaneously repels attempts at gentrification, and proves deliciously attractive to curious individuals â€“ especially younger thrill seekers. It is the Darknet without the technical blocks, and a frequent 'gateway drug' to the genuinely dangerous areas of the online world.

The central debate of Gamergate was, in the grand scheme of things, irrelevant. Suffice to say, the involved areas of the internet collapsed into hysterical arguing and flame wars, hurled a huge amount of vitriol at each other and generally achieved nothing more than a significant amount of harassment. The event itself may have been irrelevant. Its legacy however, was not. It was the first major clash between the alt-right and the alt-left within the cybersphere that penetrated into the mainstream, and the battle lines drawn in that period persist even today, even on topics such as Brexit, the US president, and so on, with remarkable â€“ though not total or immutable - consistency.

The smaller online communities were no longer politically benign. The alt-left and the establishment, with its political correctness, corruption, outdated institutions, had become an enemy of gamers and weebs, elements of which were forming what would now be recognised as the alt-right, who perceived the outside influence as an existential threat to their special interests. This sentiment which quickly morphed into a general hatred of all things related to the alt-left and the mainstream, was reciprocated with a mirror reaction occurring on the SJW aligned boards. Gamergate is vaguely akin to the Boston tea party â€“ a relatively minor event that sparks a larger movement, the flashpoint of the online culture wars. The online communities, with the huge proportion of e-culture they produced, became politicised, and directed vast amounts of effort into defaming 'libtards' and the establishment. Injustices â€“ perceived and genuine â€“ such as predatory sex gangs, political correctness, the wealth and power of big corporations in government, the failure of the establishment to tackle issues like immigration and climate change â€“ were incorporated into the narrative, fanning the embers of resentment into a raging inferno of derision and mistrust.

Meanwhile â€“ Facebook, Twitter, et al were reaching their primacy at this point, and provided the ideal platform for the smaller communities to propagate their message. It was at this point that social media and information warfare came together. The social media environment was finally primed and perfected for political messaging â€“ vast userbases on the major platforms, the ubiquity of smartphones, the increased normality and acceptance of social media, and hosts of smaller â€“ but far more active â€“ communities and individuals that were ready to take and amplify a political message. It was to these key, influential communities and individuals that the machinery of state propaganda began to direct its messaging.

Social media proved the perfect vehicle for information warfare. It removed the biggest barrier to previous information warfare â€“ that is the physical difficulty of getting the message to an audience that is often geographically far removed from the propagandist, and protected by a military and government that would do its utmost to prevent the hostile messaging getting through. In social media, one can just as easily commune with an individual in Moscow as the room next door.

Additionally, the aims of the major platforms were essentially that of information warfare itself. The business model of the social media giants after all is not connecting people to each other, but rather precision targeting advertisements at their users. Facebook is not the product â€“ the users are the product. As such, everything from the colour scheme to the page format is engineered to make the user feel relaxed and trusting â€“ there is a reason that so many social media platforms prominently feature the colour blue. Online advertisement platforms have a combined market cap of around 2 trillion USD â€“ primarily based on their ability to change people's behaviour. If disinformation can be circulated, it finds a receptive audience on a platform designed to take advantage of that.

Therefore, the true success stories in in recent times have all taken advantages of the social media environment. While brute force attempts using armies of bots and fake accounts to push a story fabricated by the propagandists â€“ such as those surrounding the shootdown of MH-17 pushed by Russia â€“ are hardly uncommon, the far more sophisticated, and generally more successful, attacks have seen the exploitation and manipulation of pre-existing sentiments, within the target population. Many such sentiments can be found within those cynical, but influential, communities of the alt-right and alt-left, primed for use by a cunning propagandist.

There are many forms of attack. The most noticeable â€“ and therefore the one that gets the most attention â€“ is a concentrated and directed attempt to push a particular narrative or story. But the more dangerous, and far more widespread form, is that of changing the core norms, and shifting the Overton window. It is very difficult to persuade a population of a mistruth. But to inject toxicity, to widen existing rifts, to turn the language from a debate to an argument â€“ that is easy to achieve, especially within the online environment. So, starting slowly, with 'satire' and jokes to soften the message - jokes often related to gaming, anime, or a tv show - and gradually normalising the concept as a legitimate viewpoint â€“ that is a very effective and destructive process.

Now â€“ as for attack and defence in information warfare: the tendency is to think about the issue with a military mentality - attack, hold, counter attack, resilience etc. This is helpful for thinking of the delivery and prevention stages of infowar, but once the attack has been successful, and the information has been introduced into the target infosphere, I find it far more helpful to think about the attack with the same mindset as one would approach a healthcare issue.

Information spreads like an infectious disease, so much so that you can effectively adapt models for the spread of a disease to that of information. Information requires transmission to spread. Historically this had to be done via either the physical movement of a human messenger, or more recently some form of mass media â€“ which still required a fair amount of infrastructure and only offered limited access to foreign states. But social media excels at spreading information, and in connecting likeminded individuals together, which massively aids transmission. Small online communities of likeminded individuals are to information warfare what uncleaned swimming pools are to a virus. As information spreads, the information mutates. When someone who has taken up an idea or concept try to relay it, they will subconsciously massage it into a form more appealing to those they are trying to spread it to. If this happens enough times, the idea or concept will have morphed into a form that is acceptable to a wider audience than the original attack. The members of the audience self-evidently know the audience far better than the propagandist will, and has the benefit of being from the 'inside', and therefore is instinctually trusted more by other members of the group. This is mimicked by sockpuppets and shills, who pose as members of the audience. There are limits of course â€“

while a minority of a population will always be receptive to most ideas, the truly abhorrent or idiotic notions have a hard time spreading, regardless of how much they change.
The healthcare mentality holds up with the response. In the same way that there is a pre-existing plan and institutions ready to deal with an outbreak of a virus, the natural defences â€“ in a liberal democracy at least â€“ for information warfare is the fourth estate. Traditionally, the debunking of falsehoods, and duty of informing the wider population has been the duty of the media. Historically, the relatively low volume, and slow spread of misinformation, meant that this was manageable. But the speed that social media allows misinformation to spread, the sheer volume of it, and the fact that trust in the media has crashed, means that this defensive system has failed in its role in recent years. Indeed, in many cases, the media have only added to the problems.
Long term, the best solution is the build up a resistance in the population to disinformation. Discernment MUST be taught in schools, to 'vaccinate' the population against future disinformation.
The grim truth of the situation is that information warfare is a weapon that is incredibly difficult for a liberal democracy to defend against. To a certain extent, it's a silver bullet against us. While the form of war is ancient, in the last decade it has reached a potency unparalleled in history. We are not ready. The tools are not easy to reach. The obvious â€“ and perhaps the most effective â€“ solutions are an anathema to societies and culture â€“ this threat needs to be taken seriously. Against the economic, technical, and military goliath that the west is, it is naÃ¯ve to think that those opposed to it would fight fair.Ã‚Ã‚Ã‚Â